arXiv:0808.3112v2 [cs.DM] 27 Sep 2008

On the decidability of semigroup freeness*

Julien Cassaigne† François Nicolas‡

September 27, 2008

Abstract

This paper deals with the decidability of semigroup freeness. More precisely, the freeness problem over a semigroup S is defined as: given a finite subset $X \subseteq S$, decide whether each element of S has at most one factorization over X. To date, the decidabilities of two freeness problems have been closely examined. In 1953, Sardinas and Patterson proposed a now famous algorithm for the freeness problem over the free monoid. In 1991, Klarner, Birget and Satterfield proved the undecidability of the freeness problem over three-by-three integer matrices. Both results led to the publication of many subsequent papers.

The aim of the present paper is three-fold: (i) to present general results concerning freeness problems, (ii) to study the decidability of freeness problems over various particular semigroups (special attention is devoted to multiplicative matrix semigroups), and (iii) to propose precise, challenging open questions in order to promote the study of the topic.

1 Introduction

We first introduces basic notation and definitions. The organization of the paper is more precisely described in Section 1.3.

As usual, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the semiring of naturals, the ring of integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively. For every integers a and b, $[\![a, b]\!]$ denotes the set of all integers n such that $a \leq n \leq b$. Unless otherwise stated, the additive and multiplicative identity elements of any semiring are simply denoted 0 and 1, respectively. The letter O denotes any matrix whose entries are all 0.

*The work was supported by the Academy of Finland under grant 204785 (Automata Theory and Combinatorics on Words). Most of the work was done while the authors were visiting the University of Turku.

†Institut de Mathématiques de Luminy, case 907, 163 avenue de Luminy, 13288 Marseille Cedex 9, France; E-mail: cassaigne@iml.univ-mrs.fr.

‡Department of Computer Science, P. O. Box 68, 00014 University of Helsinki, Finland; E-mail: nicolas@cs.helsinki.fi.

A *word* is a finite sequence of symbols called its letters. The *empty word* is denoted ε. For every word w, the *length* of w is denoted $|w|$; for every symbol a, $|w|_a$ denotes the number of occurrences of a in w. An *alphabet* is a (finite or infinite) set of symbols.

1.1 Free semigroups and codes

A *semigroup* is a set equipped with an associative binary operation. Semigroup operations are denoted multiplicatively.

Definition 1 (Code)**.** *Let S be a semigroup and let X be a subset of S. We say that X is a* code *if the property*

$$x_1 x_2 \cdots x_m = y_1 y_2 \cdots y_n \iff (x_1, x_2, \ldots, x_m) = (y_1, y_2, \ldots, y_n)$$

holds for any integers m, $n \geq 1$ and any elements x_1, x_2, $\ldots$, x_m, y_1, y_2, $\ldots$, $y_n \in X$.

Note that $(x_1, x_2, \ldots, x_m) = (y_1, y_2, \ldots, y_n)$ means that both $m = n$ and $x_i = y_i$ for every $i \in [\![1, m]\!]$. Informally, a set is not a code if and only if its elements satisfy a non-trivial equation. Or, a subset X of a semigroup S is a code if and only if no element of S has more than one factorization over X.

For every semigroup S and every subset $X \subseteq S$, X^+ denotes the closure of X under the semigroup operation: X^+ is the subsemigroup of S generated by X, and as such it is equipped with the semigroup operation induced by the operation of S.

Definition 2 (Free semigroup)**.** *A semigroup S is called* free *if there exists a code $X \subseteq S$ such that $S = X^+$.*

In other words, a semigroup is free if it is generated by a code.

A semigroup with an identity element is called a *monoid*. Many semigroups mentioned in the paper are monoids. For every monoid M and every subset $X \subseteq M$, $X^\star$ denotes the set X^+ augmented with the identity element of M. A monoid M is called *free* if there exists a code $X \subseteq M$ such that $M = X^\star$.

Remark 3. *No monoid is a free semigroup.*

The next examples illustrate the notion of code for various ground semigroups.

Let Σ be an alphabet. The set of all words over Σ is a free monoid under concatenation with the empty word as identity element and Σ as generating code. In accordance with our notation, this monoid is denoted as usual $\Sigma^\star$. The set of all non-empty words over Σ equals Σ^+. It is a free semigroup under concatenation. Both examples of free monoid and free semigroup are canonical: every free semigroup is isomorphic to Σ^+ for some alphabet Σ and every free monoid is isomorphic to $\Sigma^\star$ for some alphabet Σ (see Section 1.4).

A subset of $\Sigma^\star$ is called a *language* over Σ. In the context of combinatorics on words, the term "code" was originally introduced to denote those languages that are codes under concatenation. This particular topic has been widely studied [3].

Example 4. *Consider the semigroup* $\{\mathtt{0},\mathtt{1}\}^\star$. *The three subsets* $\{\mathtt{00},\mathtt{01},\mathtt{10},\mathtt{11}\}$, $\{\mathtt{01},\mathtt{011},\mathtt{11}\}$ *and* $\{\mathtt{0}^n\mathtt{1} : n \in \mathbb{N}\}$ *of* $\{\mathtt{0},\mathtt{1}\}^\star$ *are codes under concatenation, but* $\{\mathtt{01},\mathtt{10},\mathtt{0}\}$ *is not:* $\mathtt{0}(\mathtt{10}) = (\mathtt{01})\mathtt{0}$.

A subset $X \subseteq \Sigma^+$ is called a *prefix code* [3, Chapter 2] if for every $x \in X$ and every $s \in \Sigma^+$, $xs \notin X$. It is clear that any prefix code is a code under concatenation.

For any two semigroups S_1 and S_2, define the *direct product* of S_1 and S_2 as the Cartesian product $S_1 \times S_2$ equipped with the componentwise semigroup operation derived from the operations of S_1 and S_2: for any two elements (x_1, x_2) and (y_1, y_2) of $S_1 \times S_2$, the product $(x_1, x_2)(y_1, y_2)$ is defined as (x_1y_1, x_2y_2).

Example 5. *Consider the semigroup* $\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$. *Both subsets* $\{(\mathtt{0},\mathtt{1}),(\mathtt{1},\mathtt{0})\}$ *and* $\{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{01}),(\mathtt{01},\mathtt{10})\}$ *of* $\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$ *are codes under componentwise concatenation but* $\{(\mathtt{0},\mathtt{0}),(\mathtt{1},\mathtt{101}),(\mathtt{01},\mathtt{01})\}$ *is not:* $(\mathtt{0},\mathtt{0})(\mathtt{1},\mathtt{101})(\mathtt{01},\mathtt{01}) = (\mathtt{01},\mathtt{01})(\mathtt{0},\mathtt{0})(\mathtt{1},\mathtt{101})$.

Let $\mathbb{D}$ be a semiring, and let $\mathbb{D}^{d\times d}$ denote the set of all d-by-d matrices over $\mathbb{D}$: $\mathbb{D}^{d\times d}$ is a semigroup under usual matrix multiplication.

Example 6. *Consider the semigroup* $\mathbb{N}^{2\times 2}$. *Let* k *be an integer greater than one. The subsets*

$$\left\{ \begin{bmatrix} k & i \\ 0 & 1 \end{bmatrix} : i \in [\![0, k-1]\!] \right\}$$

and

$$\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}$$

of $\mathbb{N}^{2\times 2}$ *are codes under matrix multiplication [9] but*

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \right\}$$

is not:

$$\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} .$$

1.2 Freeness problems

The aim of the paper is to study the decidability of freeness problems over various semigroups:

Definition 7. *Let* S *be a semigroup with a recursive underlying set. The* freeness problem *over* S, *denoted* $\textsc{Free}[S]$, *is: given a finite subset* $X \subseteq S$, *decide whether* X *is a code. For every integer* $k \geq 1$, *define* $\textsc{Free}(k)[S]$ *as the following problem: given a* k*-element subset* $X \subseteq S$, *decide whether* X *is a code.*

For every integer $k \geq 1$, $\textsc{Free}(k)[S]$ is a restriction of $\textsc{Free}[S]$.

Remark 8. *Let S be a semigroup with a recursive underlying set.* $\textsc{Free}\big[S\big]$ *should not be confused with the following problem, which is not the concern of the paper: given a finite subset $X \subseteq S$, decide whether X^+ is a free semigroup. Let a, $b \in S$ be such that $\{a, b\}$ is a code: $\{a, b, ab\}$ is not a code but $\{a, b, ab\}^+$ is a free semigroup. In general, for every subset of $X \subseteq S$, the semigroup X^+ is free if and only if there exists a code $Y \subseteq X$ such that $X \subseteq Y^+$.*

Let us now present some relevant examples of freeness problems.

Example 9. *The decidability of* $\textsc{Free}\big[\Sigma^\star\big]$ *for any finite alphabet Σ was proved by Sardinas and Patterson in 1953 [41, 40, 3]. Polynomial-time algorithms were proposed afterwards [38, and references therein].*

Example 10. *For any alphabet Σ and any two distinct words x, $y \in \Sigma^\star$, $\{x, y\}$ is not a code if and only if $xy = yx$ [29]. More generally, let Σ_1, Σ_2, $\ldots$, Σ_d be d alphabets. Let $\mathbf{x}$ and $\mathbf{y}$ be two distinct elements of the semigroup $\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_d^\star$: $\mathbf{x} = (x_1, x_2, \ldots, x_d)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_d)$ where x_i and y_i belong to $\Sigma_i^\star$ for every $i \in [\![1, d]\!]$. The two-element set $\{\mathbf{x}, \mathbf{y}\}$ is not a code if and only if $x_i y_i = y_i x_i$ for each $i \in [\![1, d]\!]$. Hence,* $\textsc{Free}(2)\big[\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_d^\star\big]$ *is decidable. (In Section 7, we prove that* $\textsc{Free}(k)\big[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\big]$ *is undecidable for every integer $k \geq 13$.)*

Example 11. *For each integer $d \geq 1$,* $\textsc{Free}(1)\big[\mathbb{Q}^{d\times d}\big]$ *is decidable in polynomial time [32, Lemma 4.1] (see also Section 2). However, Klarner, Birget and Satterfield proved that* $\textsc{Free}\big[\mathbb{N}^{3\times 3}\big]$ *is undecidable. More precisely,* $\textsc{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$ *is decidable for at most finitely many positive integers k [9, 20]. (The latest undecidability result for* $\textsc{Free}\big[\mathbb{N}^{3\times 3}\big]$ *is proved in Section 7: it states that* $\textsc{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$ *is undecidable for every integer $k \geq 13$).*

1.3 Contribution

The paper is divided into eight sections.

Section 1. In the remainder of this section, we first state some useful, basic facts concerning semigroup morphisms (Section 1.4). Then, a list of previously studied problems related to the combinatorics of semigroups is presented to broaden the discussion (Section 1.5).

Section 2. A square matrix X is called torsion if there exist two positive integers p, q such that $p \neq q$ and $X^p = X^q$, or in other words if the singleton $\{X\}$ is not a code under matrix multiplication. Problems related with matrix torsion are thoroughly studied.

Section 3. For any semigroup S and any subset $X \subseteq S$, it turns out that: if X has cardinality greater that one then X is not a code if and only if the elements of X satisfy a non-trivial *balanced* equation. Section 3 explores the consequences of this result. One of them is that for every integer $k \geq 2$, $\textsc{Free}(k)\big[\mathbb{Q}^{d\times d}\big]$ is decidable if and only if $\textsc{Free}(k)\big[\mathbb{Z}^{d\times d}\big]$ is also decidable. General results concerning the decidability of freeness problems over direct products of semigroups are also obtained.

Section 4. $\text{Free}\big[\text{GL}(2,\mathbb{Z})\big]$ is shown decidable, and the freeness problem over the free group is shown decidable in polynomial time. The latter result generalizes Example 9. Both proofs are based on the same idea: over a group, the freeness problem reduces to the rational membership problem.

Section 5. We provide an example of semigroup S that does *not* satisfy a seemingly obvious property: for any integers k_1, k_2 with $1 \leq k_1 \leq k_2$, the decidability of $\text{Free}(k_2)\big[S\big]$ implies the decidability of $\text{Free}(k_1)\big[S\big]$. A weakened version of the latter statement is proved for every semigroup S with a computable operation: if $\text{Free}(k_0)\big[S\big]$ is undecidable for some integer $k_0 \geq 2$, then $\text{Free}(k)\big[S\big]$ is undecidable for infinitely many positive integers k.

Section 6. The decidability of $\text{Free}\big[\mathbb{N}^{2\times 2}\big]$ is a very exciting but difficult open question [5, 9, 26]. New ideas to tackle the problem are proposed.

Section 7. Both $\text{Free}(k)\big[\,\{\texttt{0},\texttt{1}\}^\star \times \{\texttt{0},\texttt{1}\}^\star\,\big]$ and $\text{Free}(k)\big[\mathbb{N}^{3\times 3}\big]$ are shown undecidable for every integer $k \geq 13$. The previous best undecidability bound was 14 [20].

Section 8. We complete the picture of undecidability for freeness problems over matrix semigroups: $\text{Free}(7+h)\big[\mathbb{N}^{6\times 6}\big]$, $\text{Free}(4+h)\big[\mathbb{N}^{12\times 12}\big]$, $\text{Free}(3+h)\big[\mathbb{N}^{24\times 24}\big]$ and $\text{Free}(2+h)\big[\mathbb{N}^{48\times 48}\big]$ are shown undecidable for every $h \in \mathbb{N}$. The proof technique is not new [34] but previously unpublished.

Open questions. Relevant open questions are stated all along the paper.

1.4 Semigroup morphisms

Let S and S' be two semigroups. A function $\sigma : S \to S'$ is called a *morphism* if for every x, $y \in S$, $\sigma(xy) = \sigma(x)\sigma(y)$. Note that even if both S and S' are monoids, a morphism from S to S' does not necessarily map the identity element of S to the identity element of S': throughout this paper "morphism" always means "semigroup morphism" but not necessarily "monoid morphism". Next two claims are explicitly or implicitly used many times throughout the paper.

Claim 12 (Universal property)**.** *Let Σ be an alphabet and let S be a semigroup. For any function $s : \Sigma \to S$, there exists exactly one morphism $\sigma : \Sigma^+ \to S$ such that $\sigma(a) = s(a)$ for every $a \in \Sigma$.*

Claim 13 (Injectivity criterion)**.** *Let S be a semigroup, let Σ be an alphabet and let $\sigma : \Sigma^+ \to S$ be a morphism. The morphism σ is injective if and only if it satisfies the following two properties:*

- *the restriction of σ to Σ is injective, and*
- *$\sigma(\Sigma)$ is a code.*

The free semigroup and the free monoid structures. A bijective morphism is called an *isomorphism*. The inverse function of any isomorphism is also an isomorphism. A semigroup S is free if and only if, for some alphabet Σ, there exists an isomorphism from Σ^+ onto S. A monoid M is free if and only if, for some alphabet Σ, there exists an isomorphism from $\Sigma^\star$ onto M.

Freeness problems as morphism problems. Let S be a semigroup with a recursive underlying set and let Σ be a finite alphabet. Although the set of all functions from Σ^+ to S has the power of the continuum whenever S is non-trivial, the restriction of σ to Σ provides a finite encoding of σ for any morphism $\sigma : \Sigma^+ \to S$. From now on such encodings are considered as canonical. Hence, $\textsc{Free}\big[S\big]$ can be restated as follows: given a finite alphabet Σ and a morphism $\sigma : \Sigma^+ \to S$, decide whether σ is injective. In the same way, for every positive integer k, an alternative formulation of $\textsc{Free}(k)\big[S\big]$ is: given an alphabet Σ with cardinality k and a morphism $\sigma : \Sigma^+ \to S$, decide whether σ is injective.

Substitutions. Let Σ and Δ be two alphabets. Every morphism from $\Sigma^\star$ to $\Delta^\star$ maps the empty word to itself.

For any alphabet Σ, the set of all morphisms from $\Sigma^\star$ to $\Sigma^\star$ is denoted $\hom(\Sigma^\star)$: $\hom(\Sigma^\star)$ is a monoid under function composition with the identity function as identity element. Since each morphism belonging to $\hom(\Sigma^\star)$ is naturally encoded by its restriction to Σ, $\textsc{Free}\big[\hom(\Sigma^\star)\big]$ is a well-defined computational problem.

Since $\{\mathtt{0}, \mathtt{1}\}^\star$ contains countable codes, *e.g.* the prefix code $\{\mathtt{0}^n\mathtt{1} : n \in \mathbb{N}\}$, we may state:

Claim 14. *For any finite or countable alphabet Σ, there exists an injective morphism from $\Sigma^\star$ to $\{\mathtt{0}, \mathtt{1}\}^\star$.*

1.5 Other decision problems

The decision problems that are stated in this section are related to the combinatorics of semigroups. Although they do not play any crucial role in the paper, it is interesting to compare their properties with the ones of the freeness problems.

Mortality [36]. Let S be a semigroup. A *zero element* of S is an element $z \in S$ such that $zs = sz = z$ for every $s \in S$. No semigroup has more than one zero element. For every semigroup S with a recursive underlying set and a zero element, let $\textsc{Mortal}\big[S\big]$ denote the following problem: given a finite subset $X \subseteq S$, decide whether the zero element of S belongs to X^+; for every integer $k \geq 1$, $\textsc{Mortal}(k)\big[S\big]$ denotes the restriction of $\textsc{Mortal}\big[S\big]$ to input sets X of cardinality k.

Boundedness [7]. A set $\mathcal{X}$ of matrices over the rationals is called *bounded* if there exists a positive constant M such that the absolute value of any entry of any matrix in $\mathcal{X}$

is less than M. Let $\textsc{Bounded}\big[\mathbb{Q}^{d\times d}\big]$ denote the following problem: given a finite subset $\mathcal{X} \subseteq \mathbb{Q}^{d\times d}$, decide whether $\mathcal{X}^+$ is bounded; for every integer $k \geq 1$, $\textsc{Bounded}(k)\big[\mathbb{Q}^{d\times d}\big]$ denotes the restriction of $\textsc{Bounded}(k)\big[\mathbb{Q}^{d\times d}\big]$ to input sets $\mathcal{X}$ of cardinality k.

Semigroup membership. For every semigroup S with a recursive underlying set, let $\textsc{Member}\big[S\big]$ denote the following problem: given a finite subset $X \subseteq S$ and an element $a \in S$, decide whether $a \in X^+$; for every integer $k \geq 1$, $\textsc{Member}(k)\big[S\big]$ denotes the restriction of $\textsc{Member}\big[S\big]$ to instances (X, a) such that X has cardinality k.

Semigroup finiteness. Let $\textsc{Finite}\big[S\big]$ denote the following problem: given a finite subset $X \subseteq S$, decide whether X^+ is finite; for every integer $k \geq 1$, $\textsc{Finite}(k)\big[S\big]$ denotes the restriction of $\textsc{Finite}\big[S\big]$ to input sets X of cardinality k.

Generalized Post Correspondence Problem [13]. Let GPCP denote the following problem: given two finite alphabets Σ, Δ, two morphisms σ, $\tau : \Sigma^\star \to \Delta^\star$, and four words s, s', t, $t' \in \Delta^\star$, decide whether there exists $w \in \Sigma^\star$ such that $s\sigma(w)s' = t\tau(w)t'$. For every integer $k \geq 1$, GPCP(k) denotes the restriction of GPCP to instances $(\Sigma, \Delta, \sigma, \tau, s, s', t, t')$ such that Σ has cardinality k.

2 The case of a single generator

Let S be a semigroup. An element $s \in S$ is called *torsion* if it satisfies the following four equivalent assertions.

(i). The singleton $\{s\}$ is not a code.

(ii). There exist two integers p and q with $0 < p < q$ such that $s^p = s^q$.

(iii). The semigroup $\{s, s^2, s^3, s^4, \dots\}$ has finite cardinality.

(iv). The sequence $(s, s^2, s^3, s^4, \dots)$ is eventually periodic.

For any semigroup S with a recursive underlying set, $\textsc{Free}(1)\big[S\big]$ is the complement problem of $\textsc{Finite}(1)\big[S\big]$.

2.1 Matrix torsion over the complex numbers

Next proposition characterizes those complex square matrices that are torsion.

Proposition 15. *Let d be a positive integer. For every matrix $M \in \mathbb{C}^{d\times d}$, the following four assertions are equivalent.*

(i). *The matrix M is torsion.*

(ii). *There exist $v \in [\![0, d]\!]$ and a finite set U of roots of unity such that the minimal polynomial of M over $\mathbb{C}$ equals*

$$\mathtt{z}^v \prod_{u \in U} (\mathtt{z} - u)\,.$$

(iii). *There exist a diagonal matrix D and a nilpotent matrix N satisfying: every eigenvalue of D is a root of unity and*

$$\begin{bmatrix} D & O \\ O & N \end{bmatrix}$$

is a Jordan normal form of M.

(iv). *There exists an integer $n \geq 2$ such that $M^d = M^{nd}$.*

Proof. $(i) \Rightarrow (ii)$. Assume that assertion (i) holds. Let p and q be two integers with $0 < p < q$ such that $M^p = M^q$. Let $\mu(\mathtt{z})$ denote the minimal polynomial of M over $\mathbb{C}$. Since $M^q - M^p$ is a zero matrix, $\mu(\mathtt{z})$ divides $\mathtt{z}^q - \mathtt{z}^p = \mathtt{z}^{q-p}(\mathtt{z}^p - 1)$. Hence, $\mu(\mathtt{z})$ can be written in the form $\mu(\mathtt{z}) = \mathtt{z}^v \prod_{u \in U}(\mathtt{z} - u)$ with $v \in [\![0, q-p]\!]$ and $U \subseteq \{u \in \mathbb{C} : u^p = 1\}$. Moreover, the Cayley-Hamilton theorem implies that $\mu(\mathtt{z})$ divides the characteristic polynomial of M which is of degree d. Therefore, integer v is not greater than d. We have thus shown assertion (ii).

$(ii) \Rightarrow (iii)$. The equivalence of assertions (ii) and (iii) follows from basic linear algebra.

$(iii) \Rightarrow (iv)$. Assume that assertion (iii) holds. Write M in the form

$$M = P \begin{bmatrix} D & O \\ O & N \end{bmatrix} P^{-1}\,.$$

where: P is a non-singular matrix, D is a diagonal matrix such that every eigenvalue of D is a root of unity, and N is a nilpotent matrix. Let m be a positive integer such that $\lambda^m = 1$ for every eigenvalue λ of D: D^m is an identity matrix, and thus $D^{(m+1)d} = (D^m)^d D^d = D^d$. Moreover, $N^{(m+1)d}$ and N^d are equal to the same zero matrix, and thus

$$M^{(m+1)d} = P \begin{bmatrix} D^{(m+1)d} & O \\ O & N^{(m+1)d} \end{bmatrix} P^{-1} = P \begin{bmatrix} D^d & O \\ O & N^d \end{bmatrix} P^{-1} = M^d\,.$$

Hence, assertion (iv) holds with $n := m + 1$.

$(iv) \Rightarrow (i)$. The implication $(iv) \Rightarrow (i)$ is trivial.

□

Now turn to matrices with rational entries. Next proposition characterizes those two-by-two rational matrices that are torsion.

Proposition 16. *Let i denote the imaginary unit and let $j := -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. For every matrix $M \in \mathbb{Q}^{2\times 2}$, M is torsion if and only if one the following nine matrices is a Jordan normal form of M:*

$$\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right],\ \left[\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right],\ \left[\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right],\ \left[\begin{smallmatrix}-1&0\\0&0\end{smallmatrix}\right],\ \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right],\ \left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right],\ \left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right],\ \left[\begin{smallmatrix}j&0\\0&j^2\end{smallmatrix}\right]\ \textit{or}\ \left[\begin{smallmatrix}i&0\\0&-i\end{smallmatrix}\right].$$

Proof. It is easy to check that the nine matrices listed above are torsion. The "if part" of Proposition 16 follows. Let us now prove the "only if part". Assume that M is torsion. Proposition 15 implies that M is nilpotent or diagonalizable (over the complex numbers). If M is nilpotent then either M equals $\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right]$ or $\left[\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right]$ is the Jordan normal form of M. Hence, we may assume that M is diagonalizable for the rest of the proof. Let $\chi(\mathsf{z})$ denote the characteristic polynomial of M.

First, assume that $\chi(\mathsf{z})$ is reducible over the rationals. Since $\chi(\mathsf{z})$ is of degree two, $\chi(\mathsf{z})$ splits into two linear factors, and thus M has only rational eigenvalues. Besides, Proposition 15 implies that any non-zero eigenvalue of M is a root of unity. Since -1 and $+1$ are the only rational roots of unity, the eigenvalues of M lie in the set $\{-1, 0, +1\}$. Hence, one of the following six matrices is a Jordan normal form of M: $\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-1&0\\0&0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$, or $\left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]$.

Now, assume that $\chi(\mathsf{z})$ is irreducible over the rationals. Then, $\chi(\mathsf{z})$ is a cyclotomic polynomial. Since the only two cyclotomic polynomials of degree two are $\mathsf{z}^2 + \mathsf{z} + 1 = (\mathsf{z} - j)(\mathsf{z} - j^2)$ and $\mathsf{z}^2 + 1 = (\mathsf{z} - i)(\mathsf{z} + i)$, a Jordan normal form of M is either $\left[\begin{smallmatrix}j&0\\0&j^2\end{smallmatrix}\right]$ or $\left[\begin{smallmatrix}i&0\\0&-i\end{smallmatrix}\right]$. □

Note that $\left[\begin{smallmatrix}j&0\\0&j^2\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}i&0\\0&-i\end{smallmatrix}\right]$ are the Jordan normal forms of the integer matrices $\left[\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]$, respectively.

2.2 The matrix torsion problem

Definition 17. *Define the* Matrix Torsion *problem as: given an integer $d \geq 1$ and a matrix $M \in \mathbb{Q}^{d\times d}$, decide whether M is torsion.*

The size of an instance (d, M) of Matrix Torsion equals d plus the sum of the lengths of the binary encodings over all entries of M. Note that the dimension d of the input matrix M is *not* treated as a constant.

Mandel and Simon constructed a computable function $r : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ such that for every integer $d \geq 1$ and every matrix $M \in \mathbb{Q}^{d\times d}$, $M^d = M^{d+r(d)}$ if and only if M is torsion [32]. The following two results follow:

1. Matrix Torsion is decidable, and
2. for each integer $d \geq 1$, $\mathrm{FREE}(1)\left[\mathbb{Q}^{d\times d}\right]$ is decidable in polynomial time.

However, no polynomial-time algorithm for Matrix Torsion can compute $M^{d+r(d)}$ for every instance (d, M) taken as input because r is not polynomially bounded: for every integer $d \geq 1$, $r(d)$ equals the least common multiple of all $n \in \mathbb{N} \setminus \{0\}$ such that $\phi(n) \leq d$, where ϕ denotes Euler's totient function.

Theorem 18. *The* Matrix Torsion *problem is decidable in polynomial time.*

Proof. The Matrix Power problem is: given an integer $d \geq 1$ and two matrices A, $B \in \mathbb{Q}^{d\times d}$, decide whether there exists $n \in \mathbb{N}$ such that $A^n = B$. (Note that for each integer $d \geq 1$, $\text{Member}(1)\left[\mathbb{Q}^{d\times d}\right]$ is a restriction of Matrix Power). Kannan and Lipton showed that Matrix Power is decidable in polynomial time [25]. Hence, to prove Theorem 18, it suffices to present a polynomial-time many-one reduction from Matrix Torsion to Matrix Power.

Let d be a positive integer and let $M \in \mathbb{Q}^{d\times d}$. Define two matrices A, $B \in \mathbb{Q}^{(d+2)\times(d+2)}$ by:

$$A := \begin{bmatrix} M^d & O \\ O & N_2 \end{bmatrix} \qquad \text{where} \qquad N_2 := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

and

$$B := \begin{bmatrix} M^d & O \\ O & O_2 \end{bmatrix} \qquad \text{where} \qquad O_2 := \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

It is easy to see that the instance $(d+2, A, B)$ of Matrix Power is computable in polynomial time from the instance (d, M) of Matrix Torsion. Moreover, we have $N_2^n \neq O_2$ for $n \in \{0, 1\}$, and $N_2^n = O_2$ for every integer $n \geq 2$. Hence, for every $n \in \mathbb{N}$, the following two assertions are equivalent.

(i). $A^n = B$.

(ii). $n \geq 2$ and $M^{nd} = M^d$.

Besides, Proposition 15 ensures that assertion (ii) holds for some $n \in \mathbb{N}$ if and only if M is torsion. Therefore, $(d+2, A, B)$ is a yes-instance of Matrix Power if and only if (d, M) is a yes-instance of Matrix Torsion. ☐

Since for each integer $d \geq 1$, $\text{Free}(1)\left[\mathbb{Q}^{d\times d}\right]$ is a restriction of Matrix Torsion, Theorem 18 implies that $\text{Free}(1)\left[\mathbb{Q}^{d\times d}\right]$ is decidable in polynomial time.

At this point, it is interesting to mention the following consequence of Tarski's decision procedure: given an integer $d \geq 1$ and a matrix $M \in \mathbb{Q}^{d\times d}$, it is possible to decide whether the semigroup $\{M, M^2, M^3, M^4, \dots\}$ is bounded [7].

2.3 The morphism torsion problem

Definition 19. *Define the* Morphism Torsion *problem as: given a finite alphabet* Σ *and a morphism* $\sigma \in \hom(\Sigma^\star)$*, decide whether* σ *is torsion (under function composition).*

The size of an instance (Σ, σ) of Morphism Torsion is defined as the cardinality of Σ plus the sum of the lengths of $\sigma(a)$, over all $a \in \Sigma$. Next claim states a well-known link between matrices and morphisms.

Claim 20. *Let d be a positive integer and let a_1, a_2, …, a_d be d pairwise distinct symbols. For each morphism $\sigma \in \hom(\{a_1, a_2, \ldots, a_d\}^\star)$, let P_σ denote the d-by-d integer matrix whose $(i, j)^{th}$ entry equals $|f(a_j)|_{a_i}$ for all indices i, $j \in [\![1, d]\!]$. (P_σ is usually called the* incidence matrix *of σ.)*

- (i). *Equality $P_{\sigma_1} P_{\sigma_2} = P_{\sigma_1 \sigma_2}$ holds for any two morphisms σ_1, $\sigma_2 \in \hom(\{a_1, a_2, \ldots, a_d\}^\star)$.*
- (ii). *For each matrix $P \in \mathbb{N}^{d \times d}$, there exist at most finitely many morphisms $\sigma \in \hom(\Sigma^\star)$ such that $P_\sigma = P$.*

As an application of Theorem 18, we show:

Theorem 21. *The* Morphism Torsion *problem is decidable in polynomial time.*

Proof. According to Theorem 18, it suffices to present a polynomial-time many-one reduction from Morphism Torsion to Matrix Torsion. The idea is to prove that a morphism is torsion if and only if its incidence matrix (see Claim 20) is torsion.

Let (Σ, σ) be an instance of Morphism Torsion. Let d denote the cardinality of Σ, and let P_σ denote the incidence matrix of σ as in Claim 20. (Strictly speaking, the definition of P_σ firstly requires the choice of a linear order on Σ. However, any such order is suitable for our purpose and no further mention of it is made for the rest of the proof). Now, (d, P_σ) is an instance of Matrix Torsion that is computable from (Σ, σ) in polynomial time. Let us check that (Σ, σ) is a yes-instance of Morphism Torsion if and only if (d, P_σ) is a yes-instance of Matrix Torsion.

From Claim 20(i) we deduce that $P_\sigma^n = P_{\sigma^n}$ for every $n \in \mathbb{N}$. Hence, if σ is torsion then P_σ is torsion. Conversely, assume that P_σ is torsion. Then, the set of matrices $\mathcal{P} := \{P_\sigma, P_\sigma^2, P_\sigma^3, P_\sigma^4, \ldots\}$ is finite, and thus it follows from Claim 20(ii) that there exist at most finitely many morphisms $\tau \in \hom(\Sigma^\star)$ such that $P_\tau \in \mathcal{P}$. Since P_{σ^n} is an element of $\mathcal{P}$ for every $n \in \mathbb{N}$, the set $\{\sigma, \sigma^2, \sigma^3, \sigma^4, \ldots\}$ is finite, and thus σ is torsion. □

Corollary 22. *For any finite alphabet Σ, $\text{Free}(1)\big[\hom(\Sigma^\star)\big]$ is decidable in polynomial time.*

Open question 23 (Gwénaël Richomme, private communication)**.** *The decidability of $\text{Free}(k)\big[\hom(\Sigma^\star)\big]$ is open for every alphabet Σ with cardinality greater than one and every integer k greater than one.*

3 Balanced equations

This section centers on the applications of next lemma:

Lemma 24. *Let Σ be an alphabet with cardinality greater than one, let S be a semigroup, and let $\sigma : \Sigma^+ \to S$ be a non-injective morphism. Then, there exist u, $v \in \Sigma^+$ satisfying $u \neq v$, $\sigma(u) = \sigma(v)$, and $|u|_a = |v|_a$ for every $a \in \Sigma$.*

Proof. Since σ is non-injective there exist x, $y \in \Sigma^+$ satisfying $x \neq y$ and $\sigma(x) = \sigma(y)$. If x is not a prefix of y and if y is not a prefix of x then xy and yx are clearly suitable choices for u and v, respectively. Now, assume that x is a prefix of y (the case of y is a prefix of x is symmetrical). Then, y can be written as $y = xaz$ with $a \in \Sigma$ and $z \in \Sigma^\star$. Let b be a symbol in Σ distinct from a. The words xby and ybx are suitable choices for u and v, respectively. $\square$

Colloquially, Lemma 24 means that, for any semigroup S and any subset $X \subseteq S$ such that X has cardinality greater than one, X is not a code if and only if the elements of X satisfy a non-trivial *balanced* equation.

3.1 Cancellation

Definition 25 (Cancellation)**.** *Let S be a semigroup. An element $s \in S$ is called* left-cancellative *if $su = sv$ implies $u = v$ for any u, $v \in S$. In the same way an element $t \in S$ is called* right-cancellative *if $ut = vt$ implies $u = v$ for any u, $v \in S$. An element of s that is both left-cancellative and right-cancellative is called* cancellative*.*

Example 26. *Let X be a (finite or infinite) set and let S denote the set of all functions from X to itself: S is a semigroup under function composition. The left-cancellative elements of S are the injections from X to itself, the right-cancellative elements of S are the surjections from X onto itself, and the cancellative elements of S are the bijections from X to itself.*

A useful corollary of Lemma 24 is:

Lemma 27. *Let S be a semigroup and let X be a subset of S. Assume that X has cardinality greater than one and that every element of X is left-cancellative. The set X is not a code if and only if there exist x, $y \in X$ and u, $v \in X^+$ such that $x \neq y$ and $xu = yv$.*

Proof. The "if part" is clear. Let us now prove the "only if" part. Assume that X is not a code. It follows from Lemma 24 that there exist an integer $n \geq 1$ and $2n$ elements x_1, x_2, …, x_n, y_1, y_2, …, $y_n \in X$ such that $x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_n$ and $(x_1, x_2, \ldots, x_n) \neq (y_1, y_2, \ldots, y_n)$. (In particular, Lemma 24 takes out of the way all equations of the form $wt = w$ with w, $t \in X^+$.) Let $m := \min\{i \in [\![1, n]\!] : x_i \neq y_i\}$. Equation $x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_n$ reduces to $x_m x_{m+1} \cdots x_n = y_m y_{m+1} \cdots y_n$, and thus x_m, y_m, $x_{m+1} x_{m+2} \cdots x_n$ and $y_{m+1} y_{m+2} \cdots y_n$ are suitable choices for x, y, u and v, respectively. $\square$

Lemma 27 is extensively used throughout the paper. Next proposition shows that Lemma 27 does not hold without any cancellation property.

Proposition 28. *Let*

$$X := \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix} \qquad \text{and} \qquad Y := \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} .$$

The matrix set $\{X, Y\}$ is not a code but $XU \neq YV$ holds for any U, $V \in \{X, Y\}^+$.

Proof. Since $XYXX = XXYX$, $\{X, Y\}$ is not a code. Let L denote the row matrix $\begin{bmatrix}-1 & 2\end{bmatrix}$: $LX = \begin{bmatrix}0 & 0\end{bmatrix}$ and $LY = \begin{bmatrix}3 & 6\end{bmatrix}$. On the one hand, LXU equals the zero matrix $\begin{bmatrix}0 & 0\end{bmatrix}$ and on the other hand $LYV = \begin{bmatrix}3 & 6\end{bmatrix} V$ can be written as a product of matrices with positive entries, namely $\begin{bmatrix}3 & 6\end{bmatrix}$, X and Y. From that we deduce $XU \neq YV$. □

3.2 Rational matrices versus integer matrices

Proposition 29. *Let S be a semigroup and let λ be a cancellative element of S such that λ commutes with every element of S. For any subset $X \subseteq S$ with cardinality greater than one, X is a code if and only if λX is a code (where $\lambda X := \{\lambda x : x \in X\}$).*

Proof. Let Σ be an alphabet and let $\sigma : \Sigma^+ \to S$ be a morphism such that σ induces a bijection from Σ onto X. Note that the cardinality of Σ is necessarily greater than one. Moreover, Claim 13 yields:

Claim 30. *X is a code if and only if σ is injective.*

Let $\tau : \Sigma^+ \to S$ denote the morphism given by: $\tau(a) := \lambda\sigma(a)$ for every $a \in \Sigma$. Since λ is cancellative, morphism τ induces a bijection from Σ onto λX, and thus next fact follows from Claim 13:

Claim 31. *λX is a code if and only if τ is injective.*

Since λ commutes with every element of S, $\tau(w)$ equals $\lambda^{|w|}\sigma(w)$ for every $w \in \Sigma^+$. Moreover, the cancellation property of λ ensures that, for every u, $v \in \Sigma^+$ with $|u| = |v|$, $\sigma(u) \neq \sigma(v)$ is equivalent to $\tau(u) \neq \tau(v)$. Hence, from Lemma 24 we deduce:

Claim 32. *σ is injective if and only if τ is injective.*

Proposition 29 follows from Claims 30, 31 and 32. □

Theorem 33. *Let d be a positive integer. For every integer $k \geq 2$, $\textsc{Free}(k)\left[\mathbb{Q}^{d\times d}\right]$ is decidable if and only if $\textsc{Free}(k)\left[\mathbb{Z}^{d\times d}\right]$ is decidable.*

Proof. The "only if part" is trivial since $\textsc{Free}(k)\left[\mathbb{Z}^{d\times d}\right]$ is a restriction of $\textsc{Free}(k)\left[\mathbb{Q}^{d\times d}\right]$. To prove the "if part", we present a many-one reduction from $\textsc{Free}(k)\left[\mathbb{Q}^{d\times d}\right]$ to $\textsc{Free}(k)\left[\mathbb{Z}^{d\times d}\right]$.

Let $\mathcal{X}$ be an instance $\textsc{Free}(k)\left[\mathbb{Q}^{d\times d}\right]$, *i.e.*, a k-element subset of $\mathbb{Q}^{d\times d}$. Compute a positive integer n such that $n\mathcal{X} \subseteq \mathbb{Z}^{d\times d}$, and transform $\mathcal{X}$ into $n\mathcal{X}$. It is clear that $n\mathcal{X}$ is an instance of $\textsc{Free}(k)\left[\mathbb{Z}^{d\times d}\right]$. Moreover, Proposition 29 applies with $S := \mathbb{Q}^{d\times d}$ and $\lambda := nI_d$ where I_d denotes the identity matrix of size d: $\mathcal{X}$ is a yes-instance of $\textsc{Free}(k)\left[\mathbb{Q}^{d\times d}\right]$ if and only if $n\mathcal{X}$ is a yes-instance of $\textsc{Free}(k)\left[\mathbb{Z}^{d\times d}\right]$. □

Mortality. Let $\mathcal{X}$ be a finite subset of $\mathbb{Q}^{d\times d}$ and let n be a positive integer such that $n\mathcal{X} \subseteq \mathbb{Z}^{d\times d}$: $\mathcal{X}$ is a yes-instance of $\textsc{Mortal}\big[\mathbb{Q}^{d\times d}\big]$ if and only if $n\mathcal{X}$ is a yes-instance of $\textsc{Mortal}\big[\mathbb{Z}^{d\times d}\big]$.

Hence, for every integer $k \geq 1$, $\textsc{Mortal}(k)\big[\mathbb{Q}^{d\times d}\big]$ is decidable if and only if $\textsc{Mortal}(k)\big[\mathbb{Z}^{d\times d}\big]$ is decidable. Noteworthy is that the decidability of $\textsc{Mortal}(k)\big[\mathbb{Q}^{d\times d}\big]$ is still open for several pairs (d, k) of positive integers [42, 27, 18, 8].

Boundedness. Blondel and Canterini proved that $\textsc{Bounded}(2)\big[\mathbb{Q}^{47\times 47}\big]$ is undecidable [4]. However, for every subset $\mathcal{X} \subseteq \mathbb{Z}^{d\times d}$, $\mathcal{X}$ is bounded if and only if the cardinality of $\mathcal{X}$ is finite. Hence, $\textsc{Bounded}\big[\mathbb{Z}^{d\times d}\big]$ is the same problem as $\textsc{Finite}\big[\mathbb{Z}^{d\times d}\big]$, and thus $\textsc{Bounded}\big[\mathbb{Z}^{d\times d}\big]$ is decidable for any integer $d \geq 1$ [32, 23].

Semigroup membership. There is no obvious reduction from $\textsc{Member}\big[\mathbb{Q}^{d\times d}\big]$ to $\textsc{Member}\big[\mathbb{Z}^{d\times d}\big]$. It seems impossible to preclude *a priori* the existence of an ordered pair (k_0, d_0) of positive integers satisfying: $\textsc{Member}(k_0)\big[\mathbb{Q}^{d_0\times d_0}\big]$ is undecidable while $\textsc{Member}(k_0)\big[\mathbb{Z}^{d_0\times d_0}\big]$ is decidable.

3.3 Direct products of semigroups

Lemma 34. *Let S and T be two semigroups, let X be a subset of S and let $y : X \to T$. Let Z denote the set of all ordered pairs of the form $(x, y(x))$ with $x \in X$. If T is commutative and if X has cardinality greater than one then X is a code if and only if Z is a code under componentwise semigroup operations.*

Proof. Let Σ be an alphabet and let $\sigma : \Sigma^+ \to S$ be a morphism such that σ induces a bijection from Σ onto X. The set X is a code if and only if σ is injective (Claim 13). Let $\tau : \Sigma^+ \to S \times T$ be the morphism defined by $\tau(a) := (\sigma(a), y(\sigma(a)))$ for every $a \in \Sigma$. It is clear that τ induces a bijection from Σ onto Z. Hence, τ is injective if and only if Z is a code (Claim 13). Moreover, it is also clear that

$$\tau(w) = \left(\sigma(w), \prod_{a\in\Sigma} \left(y(\sigma(a))\right)^{|w|_a}\right)$$

for every $w \in \Sigma^+$, and thus it follows from Lemma 24 that σ is injective if and only if τ is injective. $\square$

Theorem 35. *Let S and T be two semigroups whose underlying sets are both recursive, and let k be an integer greater than one.*

(i). If both S and T are non-empty and if $\textsc{Free}(k)\big[S \times T\big]$ is decidable then both $\textsc{Free}(k)\big[S\big]$ and $\textsc{Free}(k)\big[T\big]$ are decidable.

(ii). If T is commutative and if $\textsc{Free}(k)\big[S\big]$ is decidable then $\textsc{Free}(k)\big[S \times T\big]$ is decidable.

Proof. (i). Let t be an element of T. For each k-element subset $X \subseteq S$, $Z := \{(x,t) : x \in X\}$ is a k-element subset of $S \times T$, and according to Lemma 34, X is a code if and only if Z is a code. Hence, there exists a many-one reduction from $\text{FREE}(k)\big[S\big]$ to $\text{FREE}(k)\big[S \times T\big]$. In the same way, $\text{FREE}(k)\big[T\big]$ reduces to $\text{FREE}(k)\big[S \times T\big]$. This concludes the proof of point (i).

(ii). Let Z be a k-element subset of $S \times T$. Write Z in the form $Z = \{(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)\}$. If there exist two indices $i, j \in [\![1, k]\!]$ such that $i \neq j$ and $x_i = x_j$ then Z is not a code: $(x_i, y_i)(x_j, y_j) = (x_j, y_j)(x_i, y_i)$. Otherwise, $\{x_1, x_2, \ldots, x_k\}$ is a k-element subset of S, and according to Lemma 34, $\{x_1, x_2, \ldots, x_k\}$ is a code if and only if Z is a code. Hence, $\text{FREE}(k)\big[S \times T\big]$ reduces to $\text{FREE}(k)\big[S\big]$. This concludes the proof of point (ii).

□

The converse of Theorem 35(i) is false in general. Indeed, $\text{FREE}\big[\,\{\mathtt{0},\mathtt{1}\}^\star\,\big]$ is decidable while $\text{FREE}(k)\big[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\big]$ is undecidable for every integer $k \geq 13$ (see Section 7). Moreover, Theorem 35 does not hold without the assumption $k > 1$. Indeed, let T denote a commutative semigroup such that $\text{FREE}(1)\big[T\big]$ is undecidable (such a semigroup exists by Proposition 53).

(i). If S equals the free semigroup $\{\mathtt{0}\}^+$ then $\text{FREE}(1)\big[S \times T\big]$ is clearly decidable. Indeed, $\{(\mathtt{0}^n, t)\}$ is a code for every every integer $n \geq 1$ and every $t \in T$.

(ii). If S is a semigroup reduced to a singleton then $\text{FREE}(1)\big[S \times T\big]$ is undecidable.

For every $d \in \mathbb{N}$ and every semigroup S, let $S^{\times d}$ denote the semigroup obtained as the direct product of d copies of S: $S^{\times 0}$ is reduced to a singleton, $S^{\times 1} = S$, $S^{\times 2} = S \times S$, $S^{\times 3} = S \times S \times S$, *etc.* As an application of Theorem 35, we prove:

Proposition 36. *Let n be a positive integer, let Σ_1, Σ_2, $\ldots$, Σ_n be n finite alphabets, and let d denote the number of indices $i \in [\![1, n]\!]$ such that Σ_i has cardinality greater than one.*

For every integer $k \geq 1$, $\text{FREE}(k)\big[\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_n^\star\big]$ is decidable if and only if $\text{FREE}(k)\big[\,(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}\,\big]$ is decidable.

Proof. Without loss of generality, we may assume that Σ_i has cardinality greater than one for every $i \in [\![1, d]\!]$. Let S denote the semigroup $\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_d^\star$. For every $i \in [\![d+1, n]\!]$, Σ_i is empty or reduced to a singleton, and thus $\Sigma_{d+1}^\star \times \Sigma_{d+2}^\star \times \cdots \times \Sigma_n^\star$ is a commutative semigroup. Hence, it follows from Theorem 35(ii) that $\text{FREE}(k)\big[\Sigma_1^\star \times \Sigma_2^\star \times \cdots \times \Sigma_n^\star\big]$ is decidable if and only if $\text{FREE}(k)\big[S\big]$ is decidable.

For each $i \in [\![1, d]\!]$, let $\phi_i : \{\mathtt{0},\mathtt{1}\}^\star \to \Sigma_i^\star$ be an injective morphism, *e.g.* ϕ_i can be any morphism extending an injection from $\{\mathtt{0},\mathtt{1}\}$ to Σ_i. The function mapping each $(u_1, u_2, \ldots, u_d) \in (\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}$ to $(\phi_1(u_1), \phi_2(u_2), \ldots, \phi_d(u_d))$ is an injective morphism from $(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}$ to S. It induces a one-one reduction from $\text{FREE}(k)\big[\,(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}\,\big]$ to $\text{FREE}(k)\big[S\big]$.

For each $i \in [\![1, d]\!]$, let $\psi_i : \Sigma_i^\star \to \{\mathtt{0},\mathtt{1}\}^\star$ be an injective morphism (see Claim 14). The function mapping each $(v_1, v_2, \ldots, v_d) \in S$ to $(\psi_1(v_1), \psi_2(v_2), \ldots, \psi_d(v_d))$ is an injective

morphism from S to $(\{0,1\}^\star)^{\times d}$. It induces a one-one reduction from $\textsc{Free}(k)\big[S\big]$ to $\textsc{Free}(k)\big[\,(\{0,1\}^\star)^{\times d}\,\big]$. $\square$

4 Subsemigroups of groups

A *group* is a monoid in which every element is invertible. Rational subsets of groups, and in particular rational subsets of the free group, have been widely studied (see [15] and references therein). For any group G with a recursive underlying set, we prove that $\textsc{Free}\big[G\big]$ is a rational problem (Theorem 44). From this result we deduce that both $\mathrm{GL}(2,\mathbb{Z})$ and the free group have decidable freeness problems (Corollaries 46 and 50).

Remark 37. *Let G be a group with a recursive underlying set.* $\textsc{Free}\big[G\big]$ *should not be confused with the following problem, which is not the concern of the paper: given a finite subset $X \subseteq G$, decide whether the subgroup of G generated by X is a free group with basis X.*

Definition 38 (Automaton)**.** *Let X be a set. An* automaton *over X is a quadruple $A = (Q, E, I, T)$ where Q, E, I and T are finite sets satisfying $E \subseteq Q \times X \times Q$ and $I \cup T \subseteq Q$. The elements of Q are the* states *of A; the elements of E are the* transitions *of A; the elements of I are the* initial *states of A; the elements of T are the* terminal *states of A. A transition $(p, s, q) \in E$ is usually denoted $p \xrightarrow{s} q$.*

Automata over alphabets play a central role in theoretical computer science; they are termed “nondeterministic automata” or simply “automata” in most of the literature. According to our definition, an automaton over X is also an automaton over any superset of X. In particular, for any alphabet Σ, an automaton over Σ or $\Sigma \cup \{\varepsilon\}$ is also an automaton over the free monoid $\Sigma^\star$.

Definition 39 (Acceptance)**.** *Let M be a monoid, let A be an automaton over M, and let s be an element of M.*

We say that A accepts *s if for some integer $n \in \mathbb{N}$, there exist $n+1$ states q_0, q_1, …, q_n and n elements s_1, s_2, …, $s_n \in M$ meeting the following requirements: $s = s_1 s_2 \cdots s_n$, q_0 is an initial state of A, q_n is a terminal state of A, and $q_{i-1} \xrightarrow{s_i} q_i$ is a transition of A for every $i \in [\![1, n]\!]$.*

The set of all $s \in M$ such that A accepts s is denoted $\mathrm{R}(A)$.

For every automaton $A = (Q, E, I, T)$ over M such that $I \cap T \neq \emptyset$, it follows from Definition 39 that A accepts the identity element of M.

A subset of $R \subseteq M$ is called *rational* if there exists an automation A over M such that $R = \mathrm{R}(A)$. The operation of M induces a monoid operation on the power set of M: for every subsets $U, V \subseteq M$, the *product* of U and V is defined as $UV := \{uv : (u, v) \in U \times V\}$. The set of all rational subsets of M is the closure of the set of all finite subsets of M under set union, set product, and star.

Let Σ be a finite alphabet.

1. Obviously, for every automaton A over $\Sigma^\star$, there exists an automaton B over $\Sigma \cup \{\varepsilon\}$ such that $\mathrm{R}(A) = \mathrm{R}(B)$.

2. It also well-known that so called ε-transitions are disposable: for every automaton A over $\Sigma \cup \{\varepsilon\}$, there exists an automaton B over Σ such that $\mathrm{R}(A) = \mathrm{R}(B)$ [28, Chapter 4].

In both cases, B is computable from A in polynomial time. Hence, we can state:

Proposition 40. *Let Σ be a finite alphabet. For every automaton A over $\Sigma^\star$, there exists an automaton B over Σ such that $\mathrm{R}(A) = \mathrm{R}(B)$. Moreover, B is computable from A in polynomial time.*

Definition 41. *For every monoid M with a recursive underlying set, define* $\textsc{Accept}\big[M\big]$ *as the following problem: given an automaton A over M and an element $s \in M$, decide whether A accepts s.*

Note that $\textsc{Accept}\big[M\big]$ is also known as the Rational Subset problem for M [24] and as the Rational Membership problem over M [15].

Example 42. *Let Σ be finite alphabet. For an automaton A over Σ and a word $s \in \Sigma^\star$, it is possible to check in polynomial time whether A accepts s [22, Section 4.3.3]. (Note that the time complexity bound holds even if we do not assume that the automaton is* deterministic*). Hence, it follows from Proposition 40 that* $\textsc{Accept}\big[\Sigma^\star\big]$ *is decidable in polynomial time.*

Lemma 43. *Let M be a monoid with a recursive underlying set. If* $\textsc{Accept}\big[M\big]$ *is decidable then the operation of M is computable.*

Proof. For each $(x, y) \in M \times M$, define an automaton $A_{x,y}$ over M by:

- $\mathtt{I}$, $\mathtt{X}$ and $\mathtt{T}$ are the states of $A_{x,y}$;
- $\mathtt{I} \xrightarrow{x} \mathtt{X}$ and $\mathtt{X} \xrightarrow{y} \mathtt{T}$ are the transitions of $A_{x,y}$;
- $\mathtt{I}$ is the only initial state of $A_{x,y}$ and $\mathtt{T}$ is the only terminal state of $A_{x,y}$.

It clear that $\mathrm{R}(A_{x,y}) = \{xy\}$.

Now, assume that $\textsc{Accept}\big[M\big]$ is decidable. To compute xy from an input $(x, y) \in M \times M$, first compute $A_{x,y}$, and then examine the elements of M one after another until finding the one that $A_{x,y}$ accepts. $\square$

Theorem 44. *Let G be a group with a recursive underlying set.*

(i). If the function mapping each element of G to its inverse is computable in polynomial time and if $\textsc{Accept}\big[G\big]$ *is decidable in polynomial time then* $\textsc{Free}\big[G\big]$ *is decidable in polynomial time.*

(ii). If $\textsc{Accept}\big[G\big]$ *is decidable then* $\textsc{Free}\big[G\big]$ *is decidable.*

Proof. We reduce $\text{FREE}[G]$ to $\text{ACCEPT}[G]$. Let 1_G denote the identity element of G. Let X be an instance of $\text{FREE}[G]$, *i.e.*, a finite subset of G.

First, assume that X is a singleton: $X = \{x\}$ for some $x \in G$. Compute the automaton B over G defined by:

- $\mathtt{I}$ and $\mathtt{T}$ are the states of B;
- $\mathtt{I} \xrightarrow{x} \mathtt{T}$ and $\mathtt{T} \xrightarrow{1_G} \mathtt{I}$ are the transitions of B;
- $\mathtt{I}$ is the only initial state of B and $\mathtt{T}$ is the only terminal state of B.

It is clear that B is computable from x in polynomial time. Moreover B is such that $\mathrm{R}(B) = \{x\}^+$, and thus $\{x\}$ is not a code if and only if B accepts 1_G. Hence, $\text{FREE}[G]$ on singletons reduces to $\text{ACCEPT}[G]$ in polynomial time.

Now, assume that X has cardinality greater than one. Let A denote the automaton over G defined as follows:

- the states of A are $k^2 - k + 5$ in number where k denotes the cardinality of X; they are denoted $\mathtt{I}$, $\mathtt{M}$, $\mathtt{N}$, $\mathtt{P}$, $\mathtt{T}$, and $\mathtt{Q}_{x,y}$ for each ordered pair $(x, y) \in X \times X$ with $x \neq y$;
- the transitions of A are:
  - $\mathtt{I} \xrightarrow{x^{-1}} \mathtt{Q}_{x,y}$ and $\mathtt{Q}_{x,y} \xrightarrow{y} \mathtt{M}$ for each $(x, y) \in X \times X$ with $x \neq y$,
  - $\mathtt{M} \xrightarrow{x} \mathtt{N}$ for each $x \in X$ and $\mathtt{N} \xrightarrow{1_G} \mathtt{M}$,
  - $\mathtt{N} \xrightarrow{1_G} \mathtt{P}$,
  - $\mathtt{P} \xrightarrow{x^{-1}} \mathtt{T}$ for each $x \in X$ and $\mathtt{T} \xrightarrow{1_G} \mathtt{P}$;
- $\mathtt{I}$ is the only initial state of A and $\mathtt{T}$ is the only terminal state of A.

Claim 45. *For every $g \in G$, A accepts g if and only if there exist x, $y \in X$ and u, $v \in X^+$ such that $x \neq y$ and $g = x^{-1}yvu^{-1}$.*

For every x, $y \in X$ and every u, $v \in X^+$, $1_G = x^{-1}yvu^{-1}$ is equivalent to $xu = yv$. Hence, Lemma 27 and Claim 45 combine: X is not a code if and only if A accepts 1_G.

However, computing A from X requires computing x^{-1} for each $x \in X$. If the function mapping each element of G to its inverse is computable in polynomial time then A is computable from X in polynomial time, and thus point (i) holds. Now, assume that $\text{ACCEPT}[G]$ is decidable. According to Lemma 43, the operation of G is computable. Hence, it is possible to decide whether two elements of G are inverses of each other: compute their product in G and check whether it equals 1_G. Therefore, the function mapping each element of G to its inverse is computable by brute force enumeration. It follows that A is computable from X, and thus point (ii) holds. ∎

Let $\mathrm{GL}(d,\mathbb{Z})$ denote the general linear group of degree d over $\mathbb{Z}$:

$$\mathrm{GL}(d,\mathbb{Z}) = \left\{X \in \mathbb{Z}^{d\times d} : \det(X) = \pm 1\right\} .$$

Equivalently, $\mathrm{GL}(d,\mathbb{Z})$ is the set of all matrices $X \in \mathbb{Z}^{d\times d}$ such that X has an inverse in $\mathbb{Z}^{d\times d}$. It was shown by Choffrut and Karhumäki that $\textsc{Accept}\big[\mathrm{GL}(2,\mathbb{Z})\big]$ is decidable [11]. Hence, it follows from Theorem 44(ii):

Corollary 46. $\textsc{Free}\big[\mathrm{GL}(2,\mathbb{Z})\big]$ *is decidable.*

Now turn to the free group. We first introduce the notion of semi-Thue system. Semi-Thue systems are also involved in Section 7.1.

Definition 47 (Semi-Thue system)**.** *A* semi-Thue system *is a pair $T = (\Sigma, R)$ where Σ is an alphabet and where R is a subset of $\Sigma^\star \times \Sigma^\star$. The elements of R are the* rules *of T. A binary relation $\Longrightarrow_T$ over $\Sigma^\star$ is associated with T: for every x, $y \in \Sigma^\star$, $x \Longrightarrow_T y$ holds if and only if there exist $(s,t) \in R$ and z_1, $z_2 \in \Sigma^\star$ such that $x = z_1 s z_2$ and $y = z_1 t z_2$. The reflexive-transitive closure of $\Longrightarrow_T$ is denoted $\overset{\star}{\Longrightarrow}_T$.*

For the rest of the section, overlining is construed as a purely formal operation: for every alphabet Σ, $\bar{\Sigma} := \{\bar{a} : a \in \Sigma\}$ is an alphabet with the same cardinality as Σ and such that $\Sigma \cap \bar{\Sigma} = \emptyset$. Define F as the semi-Thue system

$$F := \left(\Sigma \cup \bar{\Sigma}, \left\{(a\bar{a}, \varepsilon) : a \in \Sigma\right\} \cup \left\{(\bar{a}a, \varepsilon) : a \in \Sigma\right\}\right) .$$

Let x and y be two words over $\Sigma \cup \bar{\Sigma}$. We say that x *freely reduces* to y if $x \overset{\star}{\Longrightarrow}_F y$.

Proposition 48 (Benois [15, 39])**.** *Let Σ be a finite alphabet. For every automaton A over $\Sigma \cup \bar{\Sigma}$, there exists an automaton B over $\Sigma \cup \bar{\Sigma}$ satisfying the following property: for every $x \in (\Sigma \cup \bar{\Sigma})^\star$, B accepts x if and only if A accepts a word over $\Sigma \cup \bar{\Sigma}$ that freely reduces to x. Moreover, B is computable from A in polynomial time.*

Sketch of proof. Transform A into B by applying the rules stated below until saturation. All rules apply with any states p, q, q', q'' of A and any letters a, a', $b \in \Sigma \cup \bar{\Sigma}$ such that $a' = \bar{a}$ or $a = \bar{a}'$.

Rule 1. *If both $q \xrightarrow{a} q'$ and $q' \xrightarrow{a'} q''$ are transitions of A and if q is an initial state of A then add q'' to the set of initial states of A.*

Rule 2. *If both $q \xrightarrow{a} q'$ and $q' \xrightarrow{a'} q''$ are transitions of A and if q'' is a terminal state of A then add q to the set of terminal states of A.*

Rule 3. *If $p \xrightarrow{b} q$, $q \xrightarrow{a} q'$ and $q' \xrightarrow{a'} q''$ are transitions of A then add $p \xrightarrow{b} q''$ to the set of transitions of A.*

Rule 4. *If $q \xrightarrow{a} q'$, $q' \xrightarrow{a'} q''$ and $q'' \xrightarrow{b} p$ are transitions of A then add $q \xrightarrow{b} p$ to the set of transitions of A.*

□

A word w over $\Sigma \cup \bar{\Sigma}$ is called *freely irreducible* if neither $a\bar{a}$ nor $\bar{a}a$ occurs in w for any $a \in \Sigma$. Each word over $\Sigma \cup \bar{\Sigma}$ freely reduces to a unique freely irreducible word. The *free group* over Σ is denoted $\mathrm{FG}(\Sigma)$. Its underlying set is the set of all freely irreducible words over $\Sigma \cup \bar{\Sigma}$; its operation maps each $(x, y) \in \mathrm{FG}(\Sigma) \times \mathrm{FG}(\Sigma)$ to the unique $z \in \mathrm{FG}(\Sigma)$ such that the concatenation xy freely reduces to z. The empty word is the identity element of $\mathrm{FG}(\Sigma)$, and for every $a \in \Sigma$, $\bar{a}$ is the inverse of a.

From Proposition 48 we deduce:

Corollary 49. *For any finite alphabet Σ, $\textsc{Accept}\big[\mathrm{FG}(\Sigma)\big]$ is decidable in polynomial time.*

Proof. Let A be an automaton over $\mathrm{FG}(\Sigma)$ and let $s \in \mathrm{FG}(\Sigma)$. Since $\mathrm{FG}(\Sigma)$ is a subset of $(\Sigma \cup \bar{\Sigma})^\star$, A can be seen as an automaton over $(\Sigma \cup \bar{\Sigma})^\star$. It is clear that A accepts s under the free group operation if and only if A accepts, under concatenation, a word over $\Sigma \cup \bar{\Sigma}$ that freely reduces to s. However, we can compute from A in polynomial time an automaton B over $\Sigma \cup \bar{\Sigma}$ such that: A accepts s under the free group operation if and only if B accepts s under concatenation (Propositions 40 and 48). Since the latter condition can be tested in polynomial time (see Example 42), Corollary 49 holds. □

Now, Corollary 49 together with Theorem 44 yield:

Corollary 50. *For any finite alphabet Σ, $\textsc{Free}\big[\mathrm{FG}(\Sigma)\big]$ is decidable in polynomial time.*

5 Number of generators

Let us first state two basic questions that remain unsolved.

Open question 51. *Does there exist a semigroup S_∞ with a recursive underlying set satisfying the following two properties: $\textsc{Free}(k)\big[S_\infty\big]$ is decidable for every integer $k \geq 1$, and $\textsc{Free}\big[S_\infty\big]$ is undecidable?*

Open question 52. *Let K denote the set of all integers $k \geq 1$ such that there exists a semigroup S_k with a recursive underlying set satisfying the following two properties: $\textsc{Free}(k)\big[S_k\big]$ is decidable and $\textsc{Free}(k+1)\big[S_k\big]$ is undecidable. The finiteness of K is open.*

Combining Example 11 above and Corollary 110 below, we get that $1 \in K$: $\mathbb{N}^{48\times 48}$ is a suitable choice for S_1. Combining Example 10 above and Theorem 101 below, we get that $K \cap [\![2, 12]\!] \neq \emptyset$.

Now let us address a more surprising issue. Some semigroups S with computable operations satisfy the following two apparently incompatible properties: $\textsc{Free}(1)\big[S\big]$ is undecidable whereas $\textsc{Free}(k)\big[S\big]$ is decidable for every integer $k \geq 2$.

Proposition 53. *There exists a semigroup S with a recursive underlying set such that*

- *the operation of S is commutative,*
- *the operation of S is computable, and*
- $\text{FREE}(1)\big[S\big]$ *is undecidable.*

Proof. Let L be a recursively enumerable, non-recursive language over some finite alphabet Σ. Let $(w_1, w_2, w_3, w_4, \dots)$ be a recursive enumeration of L: $L = \{w_n : n \in \mathbb{N} \setminus \{0\}\}$, and the function mapping each positive integer n to w_n is computable.

Define S as the set of all ordered pairs $(x, n) \in \Sigma^\star \times (\mathbb{N} \setminus \{0\})$ such that $x \notin \{w_1, w_2, \dots, w_{n-1}\}$, augmented with an additional element denoted $\mathtt{0}$. Note that the function mapping each positive integer n to $\{w_1, w_2, \dots, w_{n-1}\}$ is computable, and thus it is decidable whether $(x, n) \in S$ for any input pair $(x, n) \in \Sigma^\star \times (\mathbb{N} \setminus \{0\})$. For every s_1, $s_2 \in S$, define the operation $s_1 s_2$ as follows:

- if there exist $x \in \Sigma^\star$ and n_1, $n_2 \in \mathbb{N} \setminus \{0\}$ such that $s_1 = (x, n_1)$, $s_2 = (x, n_2)$ and $(x, n_1 + n_2) \in S$, then $s_1 s_2 := (x, n_1 + n_2)$,
- otherwise $s_1 s_2 := \mathtt{0}$.

Now, S is equipped with a computable, commutative, multiplicative semigroup operation.

It remains to show that $\text{FREE}(1)\big[S\big]$ is undecidable. Since L is non-recursive, it suffices to show that recognizing L reduces to deciding $\text{FREE}(1)\big[S\big]$. Each $x \in \Sigma^\star$ is transformed into the instance $\{g\}$ of $\text{FREE}(1)\big[S\big]$, where $g := (x, 1)$. We check that $\{g\}$ is a yes-instance of $\text{FREE}(1)\big[S\big]$ if and only if $x \notin L$. If $x \notin L$ then $g^n = (x, n)$ for every integer $n \geq 1$, and thus all powers of g are pairwise distinct. Conversely, assume that $x \in L$. Then, there exists an integer $p \geq 1$ such that $x = w_p$ and $x \notin \{w_1, w_2, \dots, w_{p-1}\}$. For every $n \in [\![1, p-1]\!]$, $g^n = (x, n)$, and for every integer $n \geq p$, $g^n = \mathtt{0}$: almost all powers of g are equal to $\mathtt{0}$, $\square$

For any commutative semigroup S with a recursive underlying set and any integer $k \geq 2$, $\text{FREE}(k)\big[S\big]$ trivially decidable: the problem has no yes-instance. Hence, Proposition 53 yields a semigroup with a pathological freeness problem.

Remark 54. *The semigroup S described in the proof of Proposition 53 is such that* $\text{MORTAL}(1)\big[S\big]$ *is undecidable: for every $x \in \Sigma^\star$, $x \in L$ if and only if $\{(x, 1)\}$ is a yes-instance of* $\text{MORTAL}(1)\big[S\big]$.

5.1 Regular behaviors

Proposition 53 identifies a misbehavior that seems specific to freeness problems. The aim of this section is to explain why most problems related to the combinatorics of semigroups are well-behaved.

For any set S, let $\mathcal{P}(S)$ denote the *power set* of S.

Proposition 55. *Let S be a semigroup with a recursive underlying set, let A be a recursive set, and let $\mathcal{D}$ be a subset of $\mathcal{P}(S) \times A$. For every integer $k \geq 1$, let $D(k)$ denote the following problem: given a k-element subset $X \subseteq S$ and an element $a \in A$, decide whether $(X^+, a) \in \mathcal{D}$. Let F denote the following problem: given a finite subset $X \subseteq S$ and an element $a \in A$, decide whether $(X, a) \in \mathcal{D}$.*

If the operation of S is computable and if F is decidable then one of the following two assertions hold.

(i). *$D(k)$ is decidable for every integer $k \geq 1$.*

(ii). *There exists an integer $l \geq 1$ such that for every integer $k \geq 1$, $D(k)$ is decidable if and only if $k < l$.*

Proof. It suffices to show that, for every integer $k \geq 2$, the decidability of $D(k)$ implies the decidability of $D(k-1)$.

Let (X, a) be an instance of $D(k-1)$: X is a $(k-1)$-element subset of S and a is an element of A. Compute the set $X^2 = \{xy : (x, y) \in X \times X\}$. If X^2 is a subset of X then $X^+ = X$, and thus (X, a) is a yes-instance of $D(k-1)$ if and only if (X, a) is a yes-instance of F. Assume now that X^2 is not a subset of X. Compute an element $s \in X^2$ such that $s \notin X$: $\widetilde{X} := X \cup \{s\}$ has cardinality k and $\widetilde{X}^+ = X^+$. Hence, (X, a) is a yes-instance of $D(k-1)$ if and only if $(\widetilde{X}, a)$ is a yes-instance of $D(k)$. □

Proposition 55 applies to mortality, semigroup finiteness, and semigroup boundedness problems by selecting a computable set A reduced to a singleton.

Mortality. Assume that the semigroup S has a zero element and denote it by z. Let $A := \{\texttt{padding}\}$ and let $\mathcal{D}$ be the set of all pairs $(X, \texttt{padding})$ where X is a subset of S such that $z \in X$. For every integer $k \geq 1$, $D(k)$ is equivalent to $\textsc{Mortal}(k)\big[S\big]$.

For every $M \in \mathbb{Z}^{d \times d}$, $\{M\}$ is a yes-instance of $\textsc{Mortal}(1)\big[\mathbb{Z}^{d\times d}\big]$ if and only if M^d is a zero matrix. Hence, $\textsc{Mortal}(1)\big[\mathbb{Z}^{d\times d}\big]$ is decidable for each integer $d \geq 1$. Since $\textsc{Mortal}(7)\big[\mathbb{Z}^{3\times 3}\big]$ is undecidable [20], there exists an integer $l_3 \in [\![2, 7]\!]$ such that for every integer $k \geq 1$, $\textsc{Mortal}(k)\big[\mathbb{Z}^{3\times 3}\big]$ is decidable if and only if $k < l_3$ [18]. Moreover, $\textsc{Mortal}(2)\big[\mathbb{Z}^{3l_3 \times 3l_3}\big]$ is undecidable [6, 10], and thus for every integer $k \geq 1$, $\textsc{Mortal}(k)\big[\mathbb{Z}^{3l_3 \times 3l_3}\big]$ is decidable if and only if $k = 1$.

Semigroup finiteness. If $\mathcal{D}$ is the set of all pairs $(X, \texttt{padding})$ where X is a finite subset of S, then for every integer $k \geq 1$, $D(k)$ is equivalent to $\textsc{Finite}(k)\big[S\big]$.

For any two positive integers k and d, $\textsc{Finite}(k)\big[\mathbb{Q}^{d\times d}\big]$ is decidable since the general problem $\textsc{Finite}\big[\mathbb{Q}^{d\times d}\big]$ is decidable [32, 23].

Semigroup boundedness. For each integer $d \geq 1$, let $\mathcal{D}_d$ be the set of all pairs $(X, \texttt{padding})$ where X is a bounded subset of $\mathbb{Q}^{d\times d}$. If $\mathcal{D} = \mathcal{D}_d$ for some integer $d \geq 1$ then $D(k)$ is equivalent to $\textsc{Bounded}(k)\big[\mathbb{Q}^{d\times d}\big]$ for every integer $k \geq 1$. For any integer $d \geq 1$, $\textsc{Bounded}(1)\big[\mathbb{Q}^{d\times d}\big]$ is decidable [7] while $\textsc{Bounded}(2)\big[\mathbb{Q}^{47\times 47}\big]$ is undecidable [4].

Semigroup membership. Let $A := S$ and let $\mathcal{D}$ be the set of all pairs $(X, a) \in \mathcal{P}(S) \times A$ such that $a \in X$. For every integer $k \geq 1$, $D(k)$ is exactly $\textsc{Member}(k)\big[S\big]$. For each integer $d \geq 1$, $\textsc{Member}(1)\big[\mathbb{Q}^{d\times d}\big]$ is decidable [25] whereas $\textsc{Member}(2)\big[\mathbb{Z}^{3l_3\times 3l_3}\big]$ is undecidable (mortality is clearly a special case of membership). There exist two integers l_3' and l_3'' with $2 \leq l_3'' \leq l_3' \leq l_3 \leq 7$ such that, for every integer $k \geq 1$,

- $\textsc{Member}(k)\big[\mathbb{Z}^{3\times 3}\big]$ is decidable if and only if $k < l_3'$, and
- $\textsc{Member}(k)\big[\mathbb{Q}^{3\times 3}\big]$ is decidable if and only if $k < l_3''$.

Generalized Post correspondence problem. Let $S := \{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$, let $A := \{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$, and let $\mathcal{D}$ be the set of all $(X, (s, s', t, t')) \in \mathcal{P}(S) \times A$ such that there exists $(x, y) \in X \cup \{(\varepsilon, \varepsilon)\}$ satisfying $sxs' = tyt'$. For every integer $k \geq 1$, $D(k)$ is equivalent to GPCP(k). GPCP(2) is decidable [14, 13, 19] while GPCP(5) is undecidable [20]. The decidabilities of GPCP(3) and GPCP(4) remain open.

5.2 The case of the freeness problem

Although Proposition 55 does not apply to freeness problems, the decidability of $\textsc{Free}(k+1)\big[S\big]$ might imply the decidability of $\textsc{Free}(k)\big[S\big]$ for every semigroup S with a recursive underlying set and every integer $k \geq 2$. This eventuality is supported by Theorem 61 below: if the operation of S is computable and if $\textsc{Free}(k_0)\big[S\big]$ is undecidable for some integer $k_0 \geq 2$, then $\textsc{Free}(k)\big[S\big]$ is undecidable for infinitely many positive integers k.

Definition 56 (Gadget)**.** *Let S be a semigroup. For every integer $d \geq 1$, for every element $x \in S$, and every subset $Y \subseteq S$, let $\mathrm{C}_d(x, Y)$ denote the set*

$$\{x^d\} \cup \{x^r y : (r, y) \in [\![0, d-1]\!] \times Y\} \ .$$

Note that

- $\mathrm{C}_1(x, Y) = \{x\} \cup Y$,
- $\mathrm{C}_2(x, Y) = \{x^2\} \cup Y \cup xY$,
- $\mathrm{C}_3(x, Y) = \{x^3\} \cup Y \cup xY \cup x^2Y$,
- *etc.*

Lemma 57. *Let S be a semigroup, let k be an integer greater than one, let d be a positive integer, let x be an element of S, and let Y be a $(k-1)$-element subset of S. The set $\{x\} \cup Y$ is a code of cardinality k if and only if the set $\mathrm{C}_d(x, Y)$ is a code of cardinality $1 + (k-1)d$.*

Proof. Let Σ be an alphabet with cardinality $k-1$ and let a be a symbol such that $a \notin \Sigma$. Let $\sigma : (\{a\} \cup \Sigma)^+ \to S$ be a morphism such that $\sigma(a) = x$ and $\sigma(\Sigma) = Y$.

Since $\{a\} \cup \Sigma$ has cardinality k and since $\sigma(\{a\} \cup \Sigma) = \{x\} \cup Y$, we may state:

Claim 58. *$\{x\} \cup Y$ is a code of cardinality k if and only if σ is injective.*

It is clear that $\mathrm{C}_d(a, \Sigma)$ has cardinality $1 + (k-1)d$ and that $\sigma(\mathrm{C}_d(a, \Sigma)) = \mathrm{C}_d(x, Y)$. Moreover, $\mathrm{C}_d(a, \Sigma)$ is a prefix code over $\{a\} \cup \Sigma$. Next claim follows:

Claim 59. *$\mathrm{C}_d(x, Y)$ is a code of cardinality $1 + (k-1)d$ if and only if the restriction of σ to $\mathrm{C}_d(a, \Sigma)^+$ is injective.*

The "only if" part of Lemma 57 is an immediate corollary of Claims 58 and 59. Let us now prove the "if part".

Formally, the set of all non-empty words over $\{a\} \cup \Sigma$ that do not end with a equals $(\{a\} \cup \Sigma)^\star \Sigma = \{a^n b : (n, b) \in \mathbb{N} \times \Sigma\}^+$. Moreover, let $n \in \mathbb{N}$ and $b \in \Sigma$. Write n under the form $n = qd + r$ with $q \in \mathbb{N}$ and $r \in [\![0, d-1]\!]$. Since a^d and $a^r b$ belong to $\mathrm{C}_d(a, \Sigma)$, $a^n b = (a^d)^q (a^r b)$ is an element of $\mathrm{C}_d(a, \Sigma)^+$, and thus:

Claim 60. *$(\{a\} \cup \Sigma)^\star \Sigma$ is a subset of $\mathrm{C}_d(a, \Sigma)^+$.*

Assume that σ is not injective. There exist u, $v \in (\{a\} \cup \Sigma)^+$ such that $u \neq v$ and $\sigma(u) = \sigma(v)$. Let b be an element of Σ. According to Claim 60, ub and vb are elements $\mathrm{C}_d(a, \Sigma)^+$. Since they also satisfy $ub \neq vb$ and $\sigma(ub) = \sigma(vb)$, the restriction of σ to $\mathrm{C}_d(a, \Sigma)^+$ is not injective. This concludes the proof of Lemma 57. ◻

Theorem 61. *Let S be a semigroup with a recursive underlying set such that the operation of S is computable. Let k and k' be two integers greater than one. If $k-1$ divides $k'-1$ and if $\textsc{Free}(k')[S]$ is decidable then $\textsc{Free}(k)[S]$ is decidable.*

Proof. Let X be an instance of $\textsc{Free}(k)[S]$. Pick an element $x \in X$ and compute $X' := \mathrm{C}_d(x, X \setminus \{x\})$ where $d := \frac{k'-1}{k-1}$. If X' has cardinality less than k' then Lemma 57 ensures that X is not a code. Otherwise, X' is an instance of $\textsc{Free}(k')[S]$, and Lemma 57 ensures that X is a code if and only if X' is a code. ◻

If $\textsc{Free}(k_0)[S]$ is undecidable for some integer $k_0 \geq 2$ then it follows from Theorem 61 that $\textsc{Free}(1 + (k_0 - 1)d)[S]$ is undecidable for every integer $d \geq 1$.

Corollary 62. *Let S be a semigroup with a recursive underlying set such that the operation of S is computable.*

(i). If there exists an integer $k \geq 2$ such that $\textsc{Free}(k)[S]$ is decidable then $\textsc{Free}(2)[S]$ is decidable.

(ii). If there exists an odd integer $k \geq 3$ such that $\textsc{Free}(k)[S]$ is decidable then $\textsc{Free}(3)[S]$ is decidable.

Open question 63. *Does there exist a semigroup S with a recursive underlying set and two integers k_1, k_2 with $3 \leq k_1 \leq k_2$ satisfying the following three properties: (i) the operation of S is computable, (ii) $\textsc{Free}(k_1)[S]$ is undecidable, and (iii) $\textsc{Free}(k_2)[S]$ is decidable?*

6 Two-by-two matrices

The most exciting open questions concerning the decidability of freeness problems arise from two-by-two matrix semigroups [5, 9, 26]. Noteworthy is that matrix mortality is also tricky in dimension two. In 1970, Paterson introduced $\textsc{Mortal}\left[\mathbb{Z}^{3\times 3}\right]$ and showed that the problem is undecidable [36]. Since then, the decidability of $\textsc{Mortal}\left[\mathbb{Z}^{2\times 2}\right]$ has been repeatedly reported as an open question [8, 18, 20, 27, 42]. The only partial results obtained so far are: $\textsc{Mortal}(2)\left[\mathbb{Z}^{2\times 2}\right]$ is decidable [8], and $\textsc{Mortal}\left[\mathbb{N}^{d\times d}\right]$ is decidable for each integer $d \geq 1$ [6].

6.1 Toward undecidability

Let us first introduce the field of algebraic numbers. A complex number is called an *algebraic number* if it is a root of a non-zero polynomial in one variable with rational coefficients. The set of all algebraic numbers, denoted $\overline{\mathbb{Q}}$, is a subfield of $\mathbb{C}$. More precisely, $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.

For each $u \in \overline{\mathbb{Q}}$, the *minimal polynomial* of u is defined as the unique monic polynomial over $\mathbb{Q}$ that vanishes at u and is irreducible over $\mathbb{Q}$. The *degree* of an algebraic number is defined as the degree of its minimal polynomial. Let u be an algebraic number, let d denote the degree of u and let $\mathbb{Q}(u)$ denote the smallest subfield of $\mathbb{C}$ that contains u. As a vector space over $\mathbb{Q}$, $\mathbb{Q}(u)$ is of dimension d: $(1, u, u^2, u^3, \dots, u^{d-1})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(u)$.

For computational purposes, each algebraic number u is naturally encoded by a quintuple $(\mu(\mathtt{z}), a, a', b, b')$ where:

- $\mu(\mathtt{z})$ is the minimal polynomial of u, and
- a, a', b, b' are rational numbers such that u is the unique root of $\mu(\mathtt{z})$ whose real part lies between a and a' and whose imaginary part lies between b and b'.

Under such encoding, the operations of $\overline{\mathbb{Q}}$ are computable [43].

Although the decidabilities of $\textsc{Free}\left[\mathbb{N}^{2\times 2}\right]$, $\textsc{Free}\left[\mathbb{Z}^{2\times 2}\right]$ and $\textsc{Free}\left[\mathbb{Q}^{2\times 2}\right]$ are still open, $\textsc{Free}(7)\left[L^{2\times 2}\right]$ was proven undecidable, where L denotes the ring of *Lipschitz quaternions* (or *Hamiltonian integers*) [2]. Hence, proving that $\textsc{Free}\left[\overline{\mathbb{Q}}^{2\times 2}\right]$ is undecidable could be a significant advance.

Open question 64. *Is* $\textsc{Free}\left[\overline{\mathbb{Q}}^{2\times 2}\right]$ *undecidable?*

The next lemma is folklore.

Lemma 65. *Let d be a positive integer, let $\mathbb{F}$ be a field, and let $\widehat{\mathbb{F}}$ be an extension of $\mathbb{F}$ of degree d: as a vector space over $\mathbb{F}$, $\widehat{\mathbb{F}}$ is of dimension d. There exists an injective ring homomorphism from $\widehat{\mathbb{F}}$ to $\mathbb{F}^{d\times d}$.*

Proof. Let $x \in \widehat{\mathbb{F}}$. Define the function $m_x : \widehat{\mathbb{F}} \to \widehat{\mathbb{F}}$ by: $m_x(y) := xy$ for every $y \in \widehat{\mathbb{F}}$. Colloquially, m_x is the multiplication by x in $\widehat{\mathbb{F}}$. Clearly, m_x is a $\mathbb{F}$-linear endomorphism of $\widehat{\mathbb{F}}$. Map each $x \in \widehat{\mathbb{F}}$ to the matrix representation of m_x with respect to some fixed $\mathbb{F}$-basis of $\widehat{\mathbb{F}}$: we obtain the desired ring homomorphism. $\square$

Lemma 66 ([9])**.** *Let $\mathbb{A}$ be a ring and let $\mathcal{X}$ be a subset of $\mathbb{A}^{2\times 2}$ with cardinality greater than one. If $\mathcal{X}$ is a code then for every $X \in \mathcal{X}$, the determinant of X is non-zero.*

Proof. For every $X \in \mathbb{A}^{2\times 2}$, the characteristic polynomial of X equals $\mathsf{z}^2 - \operatorname{tr}(X)\mathsf{z} + \det(X)$, where $\operatorname{tr}(X)$ denotes the *trace* of X; so the Cayley-Hamilton theorem yields:

$$X^2 - \operatorname{tr}(X)X + \det(X)\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right] = \left[\begin{smallmatrix}0 & 0\\ 0 & 0\end{smallmatrix}\right] . \tag{1}$$

Assume that there exists a matrix $X \in \mathcal{X}$ such that $\det(X) = 0$. Then X satisfies $X^2 = \operatorname{tr}(X)X$ by Equation (1). Let Y be an element of $\mathcal{X}$ distinct from X. Since both $XXYX$ and $XYXX$ are equal to $\operatorname{tr}(X)XYX$, $\mathcal{X}$ is not a code. □

For every field $\mathbb{K}$, let $\mathrm{GL}(d, \mathbb{K})$ denote the general linear group of degree d over $\mathbb{K}$:

$$\mathrm{GL}(d, \mathbb{K}) = \left\{X \in \mathbb{K}^{d\times d} : \det(X) \neq 0\right\} .$$

Proposition 67. *Let $\mathbb{K}$ be a subfield of $\overline{\mathbb{Q}}$ with a recursive underlying set.* $\textsc{Free}\left[\mathbb{K}^{2\times 2}\right]$ *is decidable if and only if* $\textsc{Free}\left[\mathrm{GL}(2, \mathbb{K})\right]$ *is decidable.*

Proof. The "only if part" is trivial since $\mathrm{GL}(2, \mathbb{K})$ is a subset of $\mathbb{K}^{2\times 2}$. Let us now prove the "if part".

Let $r : \mathbb{N}\setminus\{0\} \to \mathbb{N}\setminus\{0\}$ be a computable function such that for every integer $d \geq 1$ and every matrix $M \in \mathbb{Q}^{d\times d}$, $M^d = M^{d+r(d)}$ if and only if M is torsion [32] (see Section 2.2).

Claim 68. *Let u be an algebraic number and let d denote the degree of u. Then, u is a root of unity if and only if $u^{r(d)} = 1$.*

Claim 68 is a corollary of Lemma 65 with $\mathbb{F} := \mathbb{Q}$ and $\widehat{\mathbb{F}} := \mathbb{Q}(u)$.

Let $\mathcal{X}$ be a finite subset of $\mathbb{K}^{2\times 2}$ such that $\mathcal{X}$ is not a subset of $\mathrm{GL}(2, \mathbb{K})$. Let us explain how to decide whether $\mathcal{X}$ is a code. If $\mathcal{X}$ has cardinality greater than one then $\mathcal{X}$ is not a code by Lemma 66. Assume now that $\mathcal{X}$ has cardinality one: $\mathcal{X} = \{X\}$ for some singular matrix $X \in \mathbb{K}^{2\times 2}$. The eigenvalues of X are 0 and its trace. Therefore Proposition 15 ensures that X is torsion if and only its trace is either zero or a root of unity. Since the latter condition is decidable by Claim 68, it is decidable whether $\mathcal{X}$ is a code. □

Noteworthy is that the decidability of $\textsc{Free}\left[\mathrm{GL}(2, \mathbb{Q})\right]$ is *not* trivially implied by Corollary 46: the structure of $\mathrm{GL}(2, \mathbb{Q})$ is far more complicated than the one of $\mathrm{GL}(2, \mathbb{Z})$.

Corollary 69. *Let $\mathbb{K}$ be a subfield of $\overline{\mathbb{Q}}$ with a recursive underlying set. If* $\textsc{Free}\left[\mathbb{K}^{2\times 2}\right]$ *is undecidable then* $\textsc{Accept}\left[\mathbb{K}^{2\times 2}\right]$ *is undecidable.*

Proof. Assume that $\textsc{Accept}\left[\mathbb{K}^{2\times 2}\right]$ is decidable. Then its restriction $\textsc{Accept}\left[\mathrm{GL}(2, \mathbb{K})\right]$ is decidable. Since $\mathrm{GL}(2, \mathbb{K})$ is a group, it follows from Theorem 44(*ii*) that $\textsc{Free}\left[\mathrm{GL}(2, \mathbb{K})\right]$ is decidable. Now, Proposition 67 ensures that $\textsc{Free}\left[\mathbb{K}^{2\times 2}\right]$ is decidable. □

Open question 70. *Is* $\textsc{Accept}\left[\overline{\mathbb{Q}}^{2\times 2}\right]$ *undecidable?*

Even if the answer to Question 64 is "no", proving the undecidability of $\textsc{Accept}\left[\overline{\mathbb{Q}}^{2\times 2}\right]$ is probably much easier than proving the undecidability of $\textsc{Free}\left[\overline{\mathbb{Q}}^{2\times 2}\right]$.

6.2 Toward decidability

This section focuses on the next open question.

Open question 71 ([5, 9])**.** *Is* $\text{FREE}(2)\left[\mathbb{N}^{2\times 2}\right]$ *decidable?*

6.2.1 Two upper-triangular matrices

For each semiring $\mathbb{D}$ and each integer $d \geq 1$, let $\mathrm{Tri}(d, \mathbb{D})$ denote the set of all d-by-d upper-triangular matrices over $\mathbb{D}$. $\mathrm{Tri}(d, \mathbb{D})$ is a semigroup under usual matrix multiplication. For instance, $\mathrm{Tri}(2, \mathbb{D})$ is the set of all matrices of the form $\left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right]$ with a, b, $c \in \mathbb{D}$.

Open question 72. *Is* $\text{FREE}(2)\left[\mathrm{Tri}(2, \mathbb{N})\right]$ *decidable?*

If there exists an integer $k \geq 2$ such that $\text{FREE}(k)\left[\mathbb{N}^{2\times 2}\right]$ is decidable then $\text{FREE}(2)\left[\mathbb{N}^{2\times 2}\right]$ is decidable by Corollary 62(i). Even if the answer to Question 71 is "yes", finding an algorithm for $\text{FREE}(2)\left[\mathrm{Tri}(2, \mathbb{N})\right]$ is probably much easier than finding an algorithm for $\text{FREE}(2)\left[\mathbb{N}^{2\times 2}\right]$.

For every $\lambda \in \mathbb{Q}$, let

$$D_\lambda := \begin{bmatrix} \lambda & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad T_\lambda := \begin{bmatrix} \lambda & 1 \\ 0 & 1 \end{bmatrix} .$$

$\text{FREE}(2)\left[\mathrm{Tri}(2, \mathbb{Q})\right]$ has been solved on many instances, and it has been shown that the problem is decidable if and only if its restriction to instances of the form $\{D_\lambda, T_\mu\}$ with λ, $\mu \in \mathbb{Q} \setminus \{-1, 0, +1\}$ is also decidable [9].

Example 73 ([9])**.** *The sets* $\{D_2, T_2\}$*,* $\{D_2, T_3\}$ *and* $\left\{D_{2/7}, T_{3/4}\right\}$ *are codes under matrix multiplication.*

Example 74 ([9])**.** *The set* $\left\{D_2, T_{1/2}\right\}$ *is not a code since* $D_2 T_{1/2} = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right] = T_{1/2} D_2 T_{1/2} D_2$.

Example 75. *Let* $D := D_{2/3}$ *and* $T := T_{3/5}$*. The matrix set* $\{D, T\}$ *is not a code because both products*

$$DTTTTTTTTTTDDTDDTDDDDDDDDDD$$

and

$$TTDDDDDDTTDDTDTDTDDTTDDTDTT$$

are equal to

$$\begin{bmatrix} \frac{32768}{6591796875} & \frac{242996824}{146484375} \\ 0 & 1 \end{bmatrix} .$$

This answers an open question from [5, 9]. The result has been obtained by the mean of heavy computations. Note that D *and* T *satisfy no shorter non-trivial equation (evidence on demand).*

6.2.2 One upper-triangular and one lower-triangular matrix

For every $\lambda \in \mathbb{R}$, let

$$A_\lambda := \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad B_\lambda := \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}.$$

This section is essentially excerpted from [17]. Its focus is the set C of all $\lambda \in \mathbb{R}$ such that $\{A_\lambda, B_\lambda\}$ is a code under matrix multiplication. The restriction of $\textsc{Free}(2)\left[\mathbb{Q}^{2\times 2}\right]$ to instances of the form $\{A_\lambda, B_\lambda\}$ with $\lambda \in \mathbb{Q}$ is decidable if and only if $C \cap \mathbb{Q}$ is recursive.

Lemma 76. *Let a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 be eight real numbers, and let*

$$X := \begin{bmatrix} b_1 & b_2 \\ a_1 & a_2 \end{bmatrix} \qquad \textit{and} \qquad Y := \begin{bmatrix} a_3 & a_4 \\ b_3 & b_4 \end{bmatrix}.$$

Assume $0 \leq a_i \leq b_i$ for every $i \in \{1, 2, 3, 4\}$. Then, $\{X, Y\}$ is a code under matrix multiplication if and only if both matrices X and Y are non-singular.

Proof. The "only if part" is a consequence of Lemma 66. Let us now prove the "if part". Let $\mathcal{E}$ denote the set of all $\left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right] \in \mathbb{R}^{2\times 1}$ such that $0 < v < u$, and let $\mathcal{F}$ denote the set of all $\left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right] \in \mathbb{R}^{2\times 1}$ such that $0 < u < v$.

Assume that both X and Y are non-singular. For any two positive real numbers u and v, the column vectors $X\left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right]$ and $Y\left[\begin{smallmatrix} u \\ v \end{smallmatrix}\right]$ belong to $\mathcal{E}$ and $\mathcal{F}$, respectively. By the way of contradiction, assume that $\{X, Y\}$ is not a code. According to Lemma 27, there exist U, $V \in \{X, Y\}^+$ such that $XU = YV$. On the one hand the column vectors $XU\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ and $YV\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ are equal and on the other hand they satisfy $XU\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] \in \mathcal{E}$ and $YV\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] \in \mathcal{F}$. Since $\mathcal{E} \cap \mathcal{F} = \emptyset$, a contradiction follows. □

Proposition 77. *For every real number λ with $|\lambda| \geq 1$, $\{A_\lambda, B_\lambda\}$ is a code under matrix multiplication.*

Proof. It follows from Lemma 76 that $\{A_\lambda, B_\lambda\}$ is a code for every real number $\lambda \geq 1$. Moreover, it is easy to see that for every group G and every subset of $X \subseteq G$, X is a code if and only if $\{x^{-1} : x \in X\}$ is a code. Since $A_\lambda^{-1} = A_{-\lambda}$ and $B_\lambda^{-1} = B_{-\lambda}$ for every $\lambda \in \mathbb{R}$, $\{A_\lambda, B_\lambda\}$ is also a code for every real number $\lambda \leq -1$. □

Proposition 77 ensures that C contains every real number λ with $|\lambda| \geq 1$. Let us now prove that $\sup\left((\mathbb{R} \setminus C) \cap \mathbb{Q}\right) = 1$.

Lemma 78. *Let λ be a real number. If there exist two positive integers m and n such that*

$$\lambda^2 = \frac{mn - m - n - 1}{mn} \tag{2}$$

then $\{A_\lambda, B_\lambda\}$ is not a code under matrix multiplication.

Proof. For every m, $n \in \mathbb{Z}$, $A_\lambda^m = A_{m\lambda}$, $B_\lambda^n = B_{n\lambda}$,

$$B_\lambda A_\lambda^m B_\lambda^n A_\lambda = \begin{bmatrix} mn\lambda^2+1 & mn\lambda^3+(m+1)\lambda \\ mn\lambda^3+(n+1)\lambda & mn\lambda^4+(m+n+1)\lambda^2+1 \end{bmatrix}$$

and

$$A_\lambda B_\lambda^n A_\lambda^m B_\lambda = \begin{bmatrix} mn\lambda^4+(m+n+1)\lambda^2+1 & mn\lambda^3+(m+1)\lambda \\ mn\lambda^3+(n+1)\lambda & mn\lambda^2+1 \end{bmatrix}.$$

It follows that $B_\lambda A_\lambda^m B_\lambda^n A_\lambda = A_\lambda B_\lambda^n A_\lambda^m B_\lambda$ if and only if $mn\lambda^2+1 = mn\lambda^4+(m+n+1)\lambda^2+1$. Therefore, if both m and n are positive and if Equation (2) holds then $B_\lambda A_\lambda^m B_\lambda^n A_\lambda = A_\lambda B_\lambda^n A_\lambda^m B_\lambda$. □

It is now easy to check that $\sup(\mathbb{R} \setminus C) = 1$. Consider the special case of $m = n$ in Equation (2): for every integer $n \geq 3$,

$$\lambda_n := \frac{\sqrt{n^2-2n-1}}{n}$$

belongs to $\mathbb{R} \setminus C$ by Lemma 78 and $\lim_{n\to\infty} \lambda_n = 1$. However, λ_n is irrational for every n.

Proposition 79. *For every real number $\delta > 0$, there exists $\lambda \in \mathbb{Q}$ such that $1-\delta < \lambda < 1$ and $\{A_\lambda, B_\lambda\}$ is not a code under matrix multiplication.*

Proof. Let $(n_0, n_1, n_2, n_3, \dots)$ be the sequence of integers recursively defined by: $n_0 = 3$, $n_1 = 6$ and $n_{k+2} = 6n_{k+1} - n_k - 6$ for every $k \in \mathbb{N}$. It is easy to check that:

$$n_k = \frac{3}{4}\left(\left(3+2\sqrt{2}\right)^k + \left(3-2\sqrt{2}\right)^k\right) + \frac{3}{2}$$

for every $k \in \mathbb{N}$. Hence, n_k is positive for every $k \in \mathbb{N}$ and

$$\lambda_k := 1 - \frac{n_{k+1}+n_k+3}{2n_{k+1}n_k}$$

is a rational number that tends to one as k tends to infinity.

Now, remark that the bivariate polynomial

$$p(\mathtt{x},\mathtt{y}) := \mathtt{x}^2+\mathtt{y}^2-6\mathtt{xy}+6\mathtt{x}+6\mathtt{y}+9$$

satisfies:

$$p(6\mathtt{x}-\mathtt{y}-6,\mathtt{x}) = p(\mathtt{x},\mathtt{y}) \tag{3}$$

and

$$\left(1-\frac{\mathtt{x}+\mathtt{y}+3}{2\mathtt{xy}}\right)^2 - \frac{\mathtt{xy}-\mathtt{x}-\mathtt{y}-1}{\mathtt{xy}} = \frac{p(\mathtt{x},\mathtt{y})}{4\mathtt{x}^2\mathtt{y}^2}. \tag{4}$$

Relying on Equation (3), it is easy to check by induction that $p(n_{k+1}, n_k) = 0$ for every $k \in \mathbb{N}$. Therefore, Equation (4) ensures that

$$\lambda_k^2 = \frac{n_{k+1}n_k - n_{k+1} - n_k - 1}{n_{k+1}n_k},$$

and thus $\{A_{\lambda_k}, B_{\lambda_k}\}$ is not a code (Lemma 78). □

Let F denote the set of all $\lambda \in \mathbb{R}$ such that $\{A_\lambda, B_\lambda, A_{-\lambda}, B_{-\lambda}\}^\star$ is a free group with basis $\{A_\lambda, B_\lambda\}$. It is clear that F is a subset of C and that every transcendental number is in F. It is well known that F contains every real number λ with $|\lambda| \geq 2$ [44]. Many rational and algebraic numbers have been identified in $\mathbb{R} \setminus F$ [1, 16]: in particular, $\sup(\mathbb{R} \setminus F) = 2$ [1]. However, the existence of a rational number $\lambda \in F$ with $|\lambda| < 2$ is a long standing open question [31, page 168].

Open question 80. *Is there any rational number λ with $|\lambda| < 1$ such that $\{A_\lambda, B_\lambda\}$ is a code under matrix multiplication?*

6.3 Substitutions over the binary alphabet

Let Σ be a finite alphabet and let d denote the cardinality of Σ. Claim 20 suggests that the semigroups $\hom(\Sigma^\star)$ and $\mathbb{N}^{d\times d}$ have very similar structures. Hence, the next question is likely similar to Question 71.

Open question 81. *Is* $\textsc{Free}(2)\big[\hom(\{\mathtt{0},\mathtt{1}\}^\star)\big]$ *decidable?*

We do not know whether Question 81 is easier or harder to solve than Question 71. Anyway, let us quickly compare the two questions. First of all, next claim is a straightforward consequence of Claim 20(i).

Claim 82. *In the notation of Claim 20, let $\mathcal{S}$ be a subset of* $\hom(\{a_1, a_2, \dots, a_d\}^\star)$ *such that, for every σ, $\tau \in \mathcal{S}$, $\sigma \neq \tau \implies P_\sigma \neq P_\tau$. If $\{P_\sigma : \sigma \in \mathcal{S}\}$ is a code under matrix multiplication then $\mathcal{S}$ is a code under function composition.*

Let us now check that the converse of Claim 82 does not hold.

Proposition 83. *Let ϕ, μ, σ_1 and σ_2 be the four elements of* $\hom(\{\mathtt{0},\mathtt{1}\}^\star)$ *defined by:*

$$\begin{cases}\phi(\mathtt{0}) := \mathtt{01}\\ \phi(\mathtt{1}) := \mathtt{0}\end{cases} \qquad \begin{cases}\mu(\mathtt{0}) := \mathtt{01}\\ \mu(\mathtt{1}) := \mathtt{10}\end{cases} \qquad \begin{cases}\sigma_1(\mathtt{0}) := \mathtt{001}\\ \sigma_1(\mathtt{1}) := \mathtt{10}\end{cases} \qquad \begin{cases}\sigma_2(\mathtt{0}) := \mathtt{100}\\ \sigma_2(\mathtt{1}) := \mathtt{10}\end{cases} .$$

Both sets of morphisms $\{\phi, \mu\}$ and $\{\sigma_1, \sigma_2\}$ are codes under function composition.

Proof. It is easy to see that all four morphisms ϕ, μ, σ_1 and σ_2 are injective. Hence, ϕ, μ, σ_1 and σ_2 are left-cancellative under function composition (Example 26).

By the way of contradiction, assume that $\{\phi, \mu\}$ is not a code. Lemma 27 applies and ensures that there exist σ, $\tau \in \{\phi, \mu\}^+$ such that $\phi\sigma = \mu\tau$. Now, remark that for every $\rho \in \{\phi, \mu\}^+$, $\mathtt{01}$ is a prefix of $\rho(\mathtt{0})$. Hence, both $\phi(\mathtt{01}) = \mathtt{010}$ and $\mu(\mathtt{01}) = \mathtt{0110}$ are prefixes of $\phi(\sigma(\mathtt{0})) = \mu(\tau(\mathtt{0}))$: contradiction.

We have thus proved that $\{\phi, \mu\}$ is a code; $\{\sigma_1, \sigma_2\}$ is handled in the same way.

By the way of contradiction, assume that $\{\sigma_1, \sigma_2\}$ is not a code. Then, there exist τ_1, $\tau_2 \in \{\sigma_1, \sigma_2\}^+$ such that $\sigma_1\tau_1 = \sigma_2\tau_2$ (Lemma 27). Since $\mathtt{10}$ is a prefix of $\rho(\mathtt{1})$ for every $\rho \in \{\sigma_1, \sigma_2\}^+$, both $\sigma_1(\mathtt{10}) = \mathtt{10001}$ and $\sigma_2(\mathtt{10}) = \mathtt{10100}$ are prefixes of $\sigma_1(\tau_1(\mathtt{1})) = \sigma_2(\tau_2(\mathtt{1}))$: contradiction. $\square$

Morphisms ϕ and μ play a central role in combinatorics of words [29, 30]. They are usually called the *Fibonacci substitution* and the *Thue-Morse substitution*, respectively.

For every morphism $\sigma \in \hom(\{\mathtt{0},\mathtt{1}\}^\star)$, let us agree that the incidence matrix P_σ of σ equals:

$$\begin{bmatrix} |\sigma(\mathtt{0})|_{\mathtt{0}} & |\sigma(\mathtt{1})|_{\mathtt{0}} \\ |\sigma(\mathtt{0})|_{\mathtt{1}} & |\sigma(\mathtt{1})|_{\mathtt{1}} \end{bmatrix} .$$

The incidence matrices of ϕ, μ, σ_1 and σ_2 are:

$$P_\phi = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad P_\mu = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \qquad P_{\sigma_1} = P_{\sigma_2} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} .$$

Although $\{\phi, \mu\}$ is a code under function composition, $\{P_\phi, P_\mu\}$ is not a code under matrix multiplication: indeed P_μ is singular, and thus the contrapositive of Lemma 66 applies. Moreover, it follows from Proposition 83 that $\{\sigma_1, \sigma_2^2\}$ is a code under function composition. However, $\left\{P_{\sigma_1}, P_{\sigma_2^2}\right\} = \left\{P_{\sigma_1}, P_{\sigma_1}^2\right\}$ is not a code under matrix multiplication. Note that both P_{σ_1} and $P_{\sigma_1}^2$ are unimodular.

7 Three-by-three matrices

The aim of this section is to prove that, for every integer $k \geq 13$, both $\textsc{Free}(k)\left[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\right]$ and $\textsc{Free}(k)\left[\mathbb{N}^{3\times 3}\right]$ are undecidable. The undecidability of $\textsc{Free}(14)\left[\mathbb{N}^{3\times 3}\right]$ was recently proved by Halava, Harju and Hirvensalo [20]: building on their ideas, we improve on the result by the mean of a trick (see the proof of Theorem 99).

We first check that $\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$ is a well-behaved semigroup in the sense of Section 5.

Proposition 84. *Let k_0 be a positive integer. If $\textsc{Free}(k_0)\left[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\right]$ is decidable then for every $k \in [\![1, k_0]\!]$, $\textsc{Free}(k)\left[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\right]$ is also decidable.*

Proof. Let u, v, $w \in \{\mathtt{0},\mathtt{1}\}^\star$ be such that $\{u, v, w\}$ is a three-element code. For instance $\mathtt{1}$, $\mathtt{10}$ and $\mathtt{100}$ are suitable choices for u, v and w, respectively. Let $\sigma : \{\mathtt{0},\mathtt{1}\}^\star \to \{\mathtt{0},\mathtt{1}\}^\star$ be the morphism defined by: $\sigma(\mathtt{0}) := u$ and $\sigma(\mathtt{1}) := v$. For every subset $X \subseteq \{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$, let $X' := \{(\sigma(x), \sigma(y)) : (x, y) \in X\} \cup \{(w, w)\}$:

- if X has cardinality k then X' has cardinality $k + 1$, and
- X is a code if and only if X' is a code.

Hence, there exists a many-one reduction from $\textsc{Free}(k)\left[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\right]$ to $\textsc{Free}(k+1)\left[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\right]$. □

Note that we do not know whether Proposition 84 still holds if $\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$ is replaced with $\mathbb{N}^{3\times 3}$.

7.1 Semi-Thue systems and Post correspondence problem

In this section, we revisit Claus's many-one reduction from the accessibility problem for semi-Thue systems to the Post correspondence problem [12]. Semi-Thue systems and the notation $\overset{\star}{\Longrightarrow}$ are introduced in Definition 47.

Definition 85 (Accessibility problem for semi-Thue systems)**.** *Let* Access *denote the following problem: given a finite alphabet* Σ*, a subset* $R \subseteq \Sigma^\star \times \Sigma^\star$*, and two words* u*,* $v \in \Sigma^\star$*, decide whether* $u \overset{\star}{\Longrightarrow}_{(\Sigma,R)} v$*. For every integer* $k \geq 1$*, define* Access(k) *as the restriction of* Access *to instances* (Σ, R, u, v) *such that* R *has cardinality* k*.*

Theorem 86 (Matiyasevich and Sénizergues [33])**.** Access(3) *is undecidable.*

The decidabilities of Access(1) and Access(2) remain open.

Definition 87 (Post Correspondence Problem [37])**.** *Let* PCP *denote the following problem: given two finite alphabets* Σ*,* Δ*, and two morphisms* σ*,* $\tau : \Sigma^\star \to \Delta^\star$*, decide whether there exists* $w \in \Sigma^+$ *such that* $\sigma(w) = \tau(w)$*. For every integer* $k \geq 1$*,* PCP(k) *denotes the restriction of* PCP *to instances* $(\Sigma, \Delta, \sigma, \tau)$ *such that* Σ *has cardinality* k*.*

In 1980, Claus stated [12, Theorem 2]: if Access(k) is undecidable then PCP$(k + 4)$ is also undecidable. Hence, PCP(7) is undecidable [33]. Note in passing that PCP(2) is decidable [14, 13, 19], and that the decidabilities of PCP(3), PCP(4), PCP(5) and PCP(6) remain open. In 2007, Halava, Harju and Hirvensalo remarked [20] that the many-one reduction from Access(k) to PCP$(k+4)$ proposed by Claus [12, Theorem 2] only outputs very peculiar instances of PCP. Those instances satisfy interesting properties such as the one stated in Proposition 93.

Definition 88 (Claus instance of PCP)**.** *An instance* $(\Sigma, \Delta, \sigma, \tau)$ *of* PCP *is called a* Claus instance *if it meets the following requirements:*

- $\mathtt{b} \in \Sigma$, $\mathtt{e} \in \Sigma$, $\Delta = \{\mathtt{0}, \mathtt{1}, \mathtt{b}, \mathtt{e}, \mathtt{d}\}$,
- $\sigma(a) \in \{\mathtt{d0}, \mathtt{d1}\}^+$ *for every* $a \in \Sigma \setminus \{\mathtt{b}, \mathtt{e}\}$,
- $\tau(a) \in \{\mathtt{0d}, \mathtt{1d}\}^+$ *for every* $a \in \Sigma \setminus \{\mathtt{b}, \mathtt{e}\}$,
- $\sigma(\mathtt{b}) \in \mathtt{b}\{\mathtt{d0}, \mathtt{d1}\}^\star$,
- $\sigma(\mathtt{e}) = \{\mathtt{d0}, \mathtt{d1}\}^\star\mathtt{de}$,
- $\tau(\mathtt{b}) = \mathtt{bd}\{\mathtt{0d}, \mathtt{1d}\}^\star$, *and*
- $\tau(\mathtt{e}) \in \{\mathtt{0d}, \mathtt{1d}\}^\star\mathtt{e}$.

Definition 88 is inspired by [9, 21]. Strictly speaking, Claus's original reduction [12] does not output Claus's instances in the sense of Definition 88, but it can be easily adapted. The same holds for similar reductions doing the same job [20, 21].

Theorem 89 (Claus's theorem revisited)**.** *Let k be a positive integer. If* $\mathrm{PCP}(k+4)$ *is decidable on Claus instances then* $\textsc{Access}(k)$ *is decidable.*

A full proof Theorem 89 can be found in an unpublished paper from the second author [35]. Noteworthy is that Theorem 89 is a corollary of the following two facts:

1. if $\mathrm{GPCP}(k+2)$ is decidable then $\textsc{Access}(k)$ is decidable, and
2. if $\mathrm{PCP}(k+2)$ is decidable on Claus instances then $\mathrm{GPCP}(k)$ is decidable [21, Theorem 3.2].

Combining Theorems 86 and 89 yields:

Corollary 90 ([20])**.** $\mathrm{PCP}(7)$ *is undecidable on Claus instances.*

7.2 Mixed modification of the Post correspondence problem

Next problem is a useful link between $\textsc{Free}\left[\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\right]$ and the restriction of PCP to Claus instances.

Definition 91 (Mixed Modification of the PCP [9])**.** *Let* MMPCP *denote the following problem: given two finite alphabets Σ, Δ, and two morphisms σ, $\tau : \Sigma^\star \to \Delta^\star$, decide whether there exist an integer $n \geq 1$, n letters a_1, a_2, $\ldots$, $a_n \in \Sigma$ and $2n$ morphisms σ_1, σ_2, $\ldots$, σ_n, τ_1, τ_2, $\ldots$, $\tau_n \in \{\sigma, \tau\}$ such that*

$$\sigma_1(a_1)\sigma_2(a_2)\cdots\sigma_n(a_n) = \tau_1(a_1)\tau_2(a_2)\cdots\tau_n(a_n)$$

and

$$(\sigma_1, \sigma_2, \ldots, \sigma_n) \neq (\tau_1, \tau_2, \ldots, \tau_n) .$$

For every integer $k \geq 1$, $\mathrm{MMPCP}(k)$ *denotes the restriction of* MMPCP *to instances $(\Sigma, \Delta, \sigma, \tau)$ such that Σ has cardinality k.*

The fundamental property of MMPCP can be stated as follows:

Claim 92. *Let $(\Sigma, \Delta, \sigma, \tau)$ be an instance of* MMPCP *such that $\sigma(a) \neq \tau(a)$ for every $a \in \Sigma$. $(\Sigma, \Delta, \sigma, \tau)$ is a yes-instance of* MMPCP *if and only if $\{(\sigma(a), a) : a \in \Sigma\} \cup \{(\tau(a), a) : a \in \Sigma\}$ is not a code under componentwise concatenation.*

Let $(\Sigma, \Delta, \sigma, \tau)$ be an instance of (MM)PCP. If $(\Sigma, \Delta, \sigma, \tau)$ is a yes-instance of PCP then $(\Sigma, \Delta, \sigma, \tau)$ is a yes-instance of MMPCP. Next proposition ensures that the converse is true provided that $(\Sigma, \Delta, \sigma, \tau)$ is a Claus instance.

Proposition 93. *For every Claus instance $(\Sigma, \{\mathtt{0}, \mathtt{1}, \mathtt{b}, \mathtt{e}, \mathtt{d}\}, \sigma, \tau)$ of* MMPCP, *$(\Sigma, \{\mathtt{0}, \mathtt{1}, \mathtt{b}, \mathtt{e}, \mathtt{d}\}, \sigma, \tau)$ is a yes-instance of* MMPCP *if and only if there exists $w \in (\Sigma \setminus \{\mathtt{b}, \mathtt{e}\})^\star$ such that $\sigma(\mathtt{b}w\mathtt{e}) = \tau(\mathtt{b}w\mathtt{e})$.*

Proof. The "if part" is trivial. Let us now prove the "only if part".

Let n be a positive integer. Define $\mathcal{C}_n$ as the set of all n-tuples $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]}$ over $\Sigma \times \{\sigma, \tau\} \times \{\sigma, \tau\}$ such that

$$\sigma_1(a_1)\sigma_2(a_2)\cdots\sigma_n(a_n) = \tau_1(a_1)\tau_2(a_2)\cdots\tau_n(a_n)\,.$$

Define $\mathcal{C}'_n$ as the set of all $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]} \in \mathcal{C}_n$ such that

$$(\sigma_1, \sigma_2, \ldots, \sigma_n) \neq (\tau_1, \tau_2, \ldots, \tau_n)\,.$$

There exists a positive integer n such that $\mathcal{C}'_n \neq \emptyset$ if and only if $(\Sigma, \{\mathtt{0}, \mathtt{1}, \mathtt{b}, \mathtt{e}, \mathtt{d}\}, \sigma, \tau)$ is a yes-instance of MMPCP.

Claim 94. *For any $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]} \in \mathcal{C}'_n$, $\sigma_1 = \tau_1$ implies $(a_i, \sigma_i, \tau_i)_{i \in [\![2,n]\!]} \in \mathcal{C}'_{n-1}$.*

Claim 95. *For any $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]} \in \mathcal{C}'_n$, $\sigma_n = \tau_n$ implies $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n-1]\!]} \in \mathcal{C}'_{n-1}$.*

Lemma 96. *Let $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]} \in \mathcal{C}'_n$ and let $k \in [\![1, n-1]\!]$. If $a_k = \mathtt{e}$ or $a_{k+1} = \mathtt{b}$ then $(a_i, \sigma_i, \tau_i)_{i \in [\![1,k]\!]}$ belongs to $\mathcal{C}'_k$ or $(a_i, \sigma_i, \tau_i)_{i \in [\![k+1,n]\!]}$ belongs to $\mathcal{C}'_{n-k}$.*

Proof. We only prove the statement in the case of $a_k = \mathtt{e}$. The case of $a_{k+1} = \mathtt{b}$ is handled in the same way.

Let $s := \sigma_1(a_1)\sigma_2(a_2)\cdots\sigma_k(a_k)$ and let $t := \tau_1(a_1)\tau_2(a_2)\cdots\tau_k(a_k)$. We have $|\sigma(\mathtt{e})|_{\mathtt{e}} = |\tau(\mathtt{e})|_{\mathtt{e}} = 1$ and $|\sigma(a)|_{\mathtt{e}} = |\tau(a)|_{\mathtt{e}} = 0$ for every $a \in \Sigma \setminus \{\mathtt{e}\}$. From that we deduce:

$$|s|_{\mathtt{e}} = |a_1 a_2 \cdots a_k|_{\mathtt{e}} = |t|_{\mathtt{e}}\,. \tag{5}$$

Assume that $a_k = \mathtt{e}$. Now, both s and t end with $\mathtt{e}$. Hence, if t was a proper prefix of s then we would have $|t|_{\mathtt{e}} < |s|_{\mathtt{e}}$ in contradiction with Equation (5). In the same way s cannot be a proper prefix of t. Therefore, s equals t, and thus $(a_i, \sigma_i, \tau_i)_{i \in [\![1,k]\!]} \in \mathcal{C}_k$ and $(a_i, \sigma_i, \tau_i)_{i \in [\![k+1,n]\!]} \in \mathcal{C}_{n-k}$. ∎

Let n denote the smallest positive integer such that $\mathcal{C}'_n \neq \emptyset$. Let $(a_i, \sigma_i, \tau_i)_{i \in [\![1,n]\!]}$ be an element of $\mathcal{C}'_n$. Claim 94 ensures

$$\sigma_1 \neq \tau_1\,,$$

and since $\sigma_1(a_1)$ and $\tau_1(a_1)$ start with the same letter, we have

$$a_1 = \mathtt{b}\,.$$

In the same way, Claim 95 ensures $\sigma_n \neq \tau_n$, and since $\sigma_n(a_n)$ and $\tau_n(a_n)$ end with the same letter, we have

$$a_n = \mathtt{e}\,.$$

Furthermore, Lemma 96 ensures

$$a_i \neq \mathtt{b} \text{ and } a_i \neq \mathtt{e}$$

for every $i \in [\![2, n-1]\!]$. Hence, $w := a_2 a_3 \cdots a_{n-1}$ belongs to $(\Sigma \setminus \{\mathtt{b}, \mathtt{e}\})^\star$.

Without loss of generality, we may assume $\sigma_1 = \sigma$ and $\tau_1 = \tau$. To complete the proof of the proposition, it suffices to show that, for every $i \in [\![2, n]\!]$, $\sigma_i = \sigma$ and $\tau_i = \tau$. We proceed by induction. Let i, $j \in [\![1, n]\!]$ be such that $\sigma = \sigma_1 = \sigma_2 = \cdots = \sigma_i$ and $\tau = \tau_1 = \tau_2 = \cdots = \tau_j$.

(i). If $\sigma(a_1 a_2 \cdots a_i) = \tau(a_1 a_2 \cdots a_j)$ then $a_1 a_2 \cdots a_i = a_1 a_2 \cdots a_j = \mathtt{b}w\mathtt{e}$.

Indeed, if $\sigma(a_i)$ and $\tau(a_j)$ end with the same letter, then $a_i = a_j = \mathtt{e}$ and $i = j = n$ follows.

(ii). If $\sigma(a_1 a_2 \cdots a_i)$ is a proper prefix of $\tau(a_1 a_2 \cdots a_j)$ then $\sigma_{i+1} = \sigma$.

Indeed, assume that there exists a non-empty word s such that $\sigma(a_1 a_2 \cdots a_i)s = \tau(a_1 a_2 \cdots a_j)$. On the one hand, s starts with the same letter as $\sigma_{i+1}(a_{i+1})$. On the other hand, s belongs to $\{\mathtt{d0}, \mathtt{d1}\}^\star\mathtt{d}$ since $\sigma(a_1 a_2 \cdots a_i) \in \mathtt{b}\{\mathtt{d0}, \mathtt{d1}\}^\star$ while $\tau(a_1 a_2 \cdots a_j) \in \mathtt{bd}\{\mathtt{0d}, \mathtt{1d}\}^\star$. Hence, $\sigma_{i+1}(a_{i+1})$ starts with $\mathtt{d}$, and $\sigma_{i+1} = \sigma$ follows.

(iii). If $\tau(a_1 a_2 \cdots a_j)$ is a proper prefix of $\sigma(a_1 a_2 \cdots a_i)$ then $\tau_{j+1} = \tau$.

Point *(iii)* is proved in the same way as point *(ii)*.

□

Theorem 97 ([20])**.** MMPCP(7) *is undecidable.*

Proof. For every integer $k \geq 1$, Proposition 93 ensures that PCP(k) and MMPCP(k) are equivalent on Claus instances. Therefore, MMPCP(7) is undecidable by Corollary 90. □

Note that the decidability of MMPCP(k) remains open for each $k \in [\![2, 6]\!]$.

7.3 Proofs of the main results

We first prove that $\textsc{Free}(k)\big[\,\{\mathtt{0}, \mathtt{1}\}^\star \times \{\mathtt{0}, \mathtt{1}\}^\star\,\big]$ is undecidable for every integer $k \geq 13$. The idea is to construct a many-one reduction from MMPCP(7) on Claus instances to $\textsc{Free}(13)\big[\,\{\mathtt{0}, \mathtt{1}\}^\star \times \{\mathtt{0}, \mathtt{1}\}^\star\,\big]$.

Lemma 98. *Let S be a semigroup, let X be a subset of S, let s_1, t_1, s_2, $t_2 \in X$ and let $Y := (X \setminus \{s_1, t_1, s_2, t_2\}) \cup \{t_2 s_1, s_2 t_1, t_2 t_1\}$. If X is a code then Y is also a code.*

Proof. If X is an alphabet and if $S = X^+$ then Y is a prefix code over X. The general case follows. □

The converse of Lemma 98 is false in general. If $S = \{\mathtt{0}, \mathtt{1}, \mathtt{2}\}^+$ and if $X = \{s_1, t_1, s_2, t_2\}$ with $s_1 := \mathtt{01}$, $t_1 := \mathtt{2}$, $s_2 := \mathtt{0}$ and $t_2 := \mathtt{12}$ then $Y = \{t_2 s_1, s_2 t_1, t_2 t_1\} = \{\mathtt{1201}, \mathtt{02}, \mathtt{122}\}$ is a prefix code; however, X is not a code since $s_1 t_1 = \mathtt{012} = s_2 t_2$.

Theorem 99. *Let k be a positive integer. If* $\textsc{Free}(2k-1)\big[\,\{\mathtt{0}, \mathtt{1}\}^\star \times \{\mathtt{0}, \mathtt{1}\}^\star\,\big]$ *is decidable then both* PCP(k) *and* MMPCP(k) *are decidable on Claus instances.*

Proof. According to Proposition 93, PCP(k) and MMPCP(k) are equivalent on Claus instances.

Let $(\Sigma, \Delta, \sigma, \tau)$ be a Claus instance of MMPCP(k). Let $s_w := (\sigma(w), w)$ and $t_w := (\tau(w), w)$ for each $w \in \Sigma^\star$. Let X and Y denote the two subsets of $\Delta^\star \times \Sigma^\star$ defined by:

$$X := \{s_a : a \in \Sigma\} \cup \{t_a : a \in \Sigma\}$$

and

$$Y := (X \setminus \{s_{\mathtt{b}}, t_{\mathtt{b}}, s_{\mathtt{e}}, t_{\mathtt{e}}\}) \cup \{t_{\mathtt{e}}s_{\mathtt{b}}, s_{\mathtt{e}}t_{\mathtt{b}}, t_{\mathtt{e}}t_{\mathtt{b}}\} \ .$$

Compute two injective morphisms $\phi : \Sigma^\star \to \{\mathtt{0}, \mathtt{1}\}^\star$ and $\psi : \Delta^\star \to \{\mathtt{0}, \mathtt{1}\}^\star$ (see Claim 14), and let

$$Z := \{(\psi(y_1), \phi(y_2)) : (y_1, y_2) \in Y\} \ .$$

Lemma 100. *If $\sigma(a) \neq \tau(a)$ for every $a \in \Sigma$ then the following four assertions are equivalent.*

(i). $(\Sigma, \Delta, \sigma, \tau)$ is a yes-instance of MMPCP(k)*.*

(ii). X is not a code.

(iii). Y is not a code.

(iv). Z is not a code.

Proof. Trivially, (iii) and (iv) are equivalent. By Claim 92, (i) and (ii) are equivalent. By Lemma 98, (iii) implies (ii).

Assume that $(\Sigma, \Delta, \sigma, \tau)$ is a yes-instance of MMPCP(k). By Lemma 93, there exists $w \in (\Sigma \setminus \{\mathtt{b}, \mathtt{e}\})^\star$ such that $\sigma(\mathtt{b}w\mathtt{e}) = \tau(\mathtt{b}w\mathtt{e})$. The word w satisfies $s_{\mathtt{b}}s_w s_{\mathtt{e}} = s_{\mathtt{b}w\mathtt{e}} = t_{\mathtt{b}w\mathtt{e}} = t_{\mathtt{b}}t_w t_{\mathtt{e}}$, and thus we have

$$(t_{\mathtt{e}}s_{\mathtt{b}})s_w(s_{\mathtt{e}}t_{\mathtt{b}}) = (t_{\mathtt{e}}t_{\mathtt{b}})t_w(t_{\mathtt{e}}t_{\mathtt{b}}) \, . \tag{6}$$

Since $t_{\mathtt{e}}s_{\mathtt{b}} \in Y$, $t_{\mathtt{e}}t_{\mathtt{b}} \in Y$, $s_w(s_{\mathtt{e}}t_{\mathtt{b}}) \in Y^+$, $t_w(t_{\mathtt{e}}t_{\mathtt{b}}) \in Y^+$ and $t_{\mathtt{e}}s_{\mathtt{b}} \neq t_{\mathtt{e}}t_{\mathtt{b}}$, Equation (6) ensures that Y is not a code. Therefore, (i) implies (iii). This concludes the proof of Lemma 100. □

It is clear that X, Y and Z are computable from $(\Sigma, \Delta, \sigma, \tau)$. If there exists $a \in \Sigma$ such that $\sigma(a) = \tau(a)$ then $(\Sigma, \Delta, \sigma, \tau)$ is a yes-instance of MMPCP(k). Conversely, let us assume $\sigma(a) \neq \tau(a)$ for every $a \in \Sigma$. Now, X has cardinality $2k$, Y has cardinality $2k - 1$ and Z is an instance of $\textsc{Free}(2k-1)\big[\,\{\mathtt{0}, \mathtt{1}\}^\star \times \{\mathtt{0}, \mathtt{1}\}^\star\,\big]$. Moreover, Lemma 100 ensures that solving MMPCP(k) on $(\Sigma, \Delta, \sigma, \tau)$ reduces to deciding whether Z is a code. □

Corollary 101. *For every integer $k \geq 13$, $\textsc{Free}(k)\big[\,\{\mathtt{0}, \mathtt{1}\}^\star \times \{\mathtt{0}, \mathtt{1}\}^\star\,\big]$ is undecidable.*

Proof. Combining Corollary 90 and Theorem 99, we obtain that $\textsc{Free}(13)\big[\,\{\mathtt{0}, \mathtt{1}\}^\star \times \{\mathtt{0}, \mathtt{1}\}^\star\,\big]$ is undecidable. Hence, the corollary holds by Proposition 84. □

By way of digression, we briefly summarize the current knowledge about the decidability of $\textsc{Free}(k)\left[\,(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}\,\right]$ for all k, $d \in \mathbb{N} \setminus \{0\}$. On the one hand, $\textsc{Free}(k)\left[\,\{\mathtt{0},\mathtt{1}\}^\star\,\right]$ is decidable for every integer $k \geq 1$ [40, 3, 38], and so is $\textsc{Free}(2)\left[\,(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}\,\right]$ for every integer $d \geq 1$ (Example 10). On the other hand, if $\textsc{Free}(k)\left[\,(\{\mathtt{0},\mathtt{1}\}^\star)^{\times (d+1)}\,\right]$ is decidable then $\textsc{Free}(k)\left[\,(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}\,\right]$ is also decidable. Indeed, there exist injective morphisms from $(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}$ to $(\{\mathtt{0},\mathtt{1}\}^\star)^{\times (d+1)}$: for instance, the function mapping each d-tuple $(u_1, u_2, \ldots, u_d)$ over $\{\mathtt{0},\mathtt{1}\}^\star$ to $(u_1, u_2, \ldots, u_d, \varepsilon)$. Hence, it follows from Corollary 101 that $\textsc{Free}(k)\left[\,(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}\,\right]$ is undecidable for every $(k, d) \in (\mathbb{N} \setminus [\![0, 12]\!]) \times (\mathbb{N} \setminus \{0, 1\})$.

Open question 102. *The decidability of* $\textsc{Free}(k)\left[\,(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}\,\right]$ *is open for every* $(k, d) \in [\![3, 12]\!] \times (\mathbb{N} \setminus \{0, 1\})$.

Let us now return to our main plot. It remains to prove that $\textsc{Free}(k)\left[\mathbb{N}^{3\times 3}\right]$ is undecidable for every integer $k \geq 13$,

Lemma 103 ([36], [9, Section 3], [20, Lemma 2], *etc*)**.** *There exists an injective morphism from* $\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$ *to* $\mathbb{N}^{3\times 3}$.

Proof. Let $\beta : \{\mathtt{0},\mathtt{1}\}^\star \to \mathbb{N}$ be the function defined by: $\beta(\mathtt{0}) = 0$, $\beta(\mathtt{1}) = 1$, and $\beta(uv) = \beta(u) + 2^{|u|}\beta(v)$ for every u, $v \in \{\mathtt{0},\mathtt{1}\}^\star$. The word $a_n \cdots a_3 a_2 a_1$ is a binary expansion of the natural number $\beta(a_1 a_2 a_3 \cdots a_n)$ for any integer $n \geq 1$ and any a_1, a_2, a_3, $\ldots$, $a_n \in \{\mathtt{0},\mathtt{1}\}$. Define $\Phi : \{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star \to \mathbb{N}^{3\times 3}$ by:

$$\Phi(u, v) := \begin{bmatrix} 2^{|u|} & 0 & \beta(u) \\ 0 & 2^{|v|} & \beta(v) \\ 0 & 0 & 1 \end{bmatrix}$$

for every u, $v \in \{\mathtt{0},\mathtt{1}\}^\star$. It is easy to check that Φ is a morphism: $\Phi(u_1u_2, v_1v_2) = \Phi(u_1, v_1)\Phi(u_2, v_2)$ for every u_1, u_2, v_1, $v_2 \in \{\mathtt{0},\mathtt{1}\}^\star$. Note that β is not injective since $\beta(u) = \beta(u\mathtt{0})$ for every $u \in \{\mathtt{0},\mathtt{1}\}^\star$. However, any $u \in \{\mathtt{0},\mathtt{1}\}^\star$ is completely determined by the pair $(|u|, \beta(u))$. Hence, Φ is injective. □

Lemma 103 can be easily generalized to higher dimensions: for every integer $d \geq 1$, there exists an injective morphism from $(\{\mathtt{0},\mathtt{1}\}^\star)^{\times d}$ to $\mathbb{N}^{(d+1)\times(d+1)}$. However, there is no injective injective morphism from $\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$ to $\mathbb{C}^{2\times 2}$ [9].

Theorem 104. *Let k be a positive integer. If* $\textsc{Free}(k)\left[\mathbb{N}^{3\times 3}\right]$ *is decidable then* $\textsc{Free}(k)\left[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\right]$ *is decidable.*

Proof. Any injective morphism from $\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star$ to $\mathbb{N}^{3\times 3}$ induces a one-one reduction from $\textsc{Free}(k)\left[\,\{\mathtt{0},\mathtt{1}\}^\star \times \{\mathtt{0},\mathtt{1}\}^\star\,\right]$ to $\textsc{Free}(k)\left[\mathbb{N}^{3\times 3}\right]$. Hence, Theorem 104 follows from Lemma 103. □

From Corollary 101 and Theorem 104 we deduce:

Corollary 105. *For every integer $k \geq 13$,* $\textsc{Free}(k)\left[\mathbb{N}^{3\times 3}\right]$ *is undecidable.*

8 Matrices of higher dimension

The main aim of this section is to prove that $\textsc{Free}(2)\left[\mathbb{N}^{d\times d}\right]$ is undecidable for some integer $d \geq 1$. Although the result is not new [34], it has never been published before.

Theorem 106. *Let $\mathbb{D}$ be a semiring with a recursive underlying set and let k be a positive integer. If $\textsc{Free}(k)\left[\mathbb{D}^{2\times 2}\right]$ is decidable then $\textsc{Free}(2k-1)\left[\mathbb{D}\right]$ is decidable.*

Proof. We present a many-one reduction from $\textsc{Free}(2k-1)\left[\mathbb{D}\right]$ to $\textsc{Free}(k)\left[\mathbb{D}^{2\times 2}\right]$. The construction is the same as in [34].

Let X be a $(2k-1)$-element subset of $\mathbb{D}$. Write X in the form:

$$X = \{x, y_1, y_2, \ldots, y_{k-1}, z_1, z_2, \ldots, z_{k-1}\} .$$

Let

$$M := \begin{bmatrix} 0 & x \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad N_i := \begin{bmatrix} 0 & z_i \\ 0 & y_i \end{bmatrix}$$

for each $i \in [\![1, k-1]\!]$. Now,

$$\mathcal{X} := \{M, N_1, N_2, \ldots, N_{k-1}\}$$

is a k-element subset of $\mathbb{D}^{2\times 2}$, and $\mathcal{X}$ is computable from X. To complete the proof, it remains to check the correctness statement: X is a code under the multiplicative operation of $\mathbb{D}$ if and only if $\mathcal{X}$ is a code under matrix multiplication.

An instance of the gadget introduced in Definition 56 plays central role in the proof: let

$$\mathcal{C} := \mathrm{C}_2\left(M, \{N_1, N_2, \ldots, N_{k-1}\}\right) = \left\{M^2, N_1, N_2, \ldots, N_{k-1}, MN_1, MN_2, \ldots, MN_{k-1}\right\} .$$

Let $\phi : \mathbb{D}^{2\times 2} \to \mathbb{D}$ be the function defined by:

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) := d$$

for every a, b, c, $d \in \mathbb{D}$. Straightforward computations yield

$$\phi(M^2) = x\,, \qquad \phi(N_i) = y_i\,, \qquad \text{and} \qquad \phi(MN_i) = z_i$$

for every $i \in [\![1, k-1]\!]$. Hence, ϕ induces a bijection from $\mathcal{C}$ onto X. In particular, $\mathcal{C}$ has cardinality $2k-1$, and thus Lemma 57 yields:

Claim 107. *$\mathcal{X}$ is a code if and only if $\mathcal{C}$ is a code.*

Recall that $\mathrm{Tri}(2, \mathbb{D})$ denotes the set of all two-by-two upper triangular matrices over $\mathbb{D}$ (see Section 6.2.1). Remark that ϕ induces a morphism from $\mathrm{Tri}(2, \mathbb{D})$ to $\mathbb{D}$ and that $\mathcal{C} \subseteq \mathrm{Tri}(2, \mathbb{D})$. If some element of $\mathcal{C}^+$ has more than one factorization over $\mathcal{C}$ then its image under ϕ has more than one factorization over X. From that we deduce:

Claim 108. *If X is a code then $\mathcal{C}$ is a code.*

Let $\mathcal{N}$ denote the set of all matrices of the form $\left[\begin{smallmatrix} 0 & u \\ 0 & v \end{smallmatrix}\right]$ with u, $v \in \mathbb{D}$. For every $i \in [\![1, k-1]\!]$ and every $N \in \mathcal{N}$, straightforward computations yield

$$NM^2 = Nx\,, \qquad NN_i = Ny_i, \qquad \text{and} \qquad NMN_i = Nz_i\,.$$

It follows that for every $N \in \mathcal{N}$ and every $P \in \mathcal{C}^+$, $NP = N\phi(P)$. Since $N_1 \in \mathcal{N}$, every P, $Q \in \mathcal{C}^+$ such that $\phi(P) = \phi(Q)$ satisfy also $N_1P = N_1Q$. Hence, under the assumption that $\mathcal{C}$ is a code, the morphism ϕ is injective on $\mathcal{C}^+$ because N_1 is cancellative in $\mathcal{C}^+$. From that we deduce:

Claim 109. *If $\mathcal{C}$ is a code then X is a code.*

Claims 107, 108 and 109 imply the correctness statement. □

Corollary 110. *For every $h \in \mathbb{N}$, $\text{Free}(7+h)\left[\mathbb{N}^{6\times 6}\right]$, $\text{Free}(4+h)\left[\mathbb{N}^{12\times 12}\right]$, $\text{Free}(3+h)\left[\mathbb{N}^{24\times 24}\right]$, and $\text{Free}(2+h)\left[\mathbb{N}^{48\times 48}\right]$ are undecidable.*

Proof. Let k, d be two positive integers. Apply Theorem 106 with $\mathbb{D} := \mathbb{N}^{d\times d}$ and identify $\left(\mathbb{N}^{d\times d}\right)^{2\times 2}$ with $\mathbb{N}^{2d\times 2d}$: if $\text{Free}(2k-1)\left[\mathbb{N}^{d\times d}\right]$ is undecidable then $\text{Free}(k)\left[\mathbb{N}^{2d\times 2d}\right]$ is undecidable. Hence, Corollary 110 follows from Corollary 105. □

In particular, $\text{Free}(2)\left[\mathbb{N}^{48\times 48}\right]$ is undecidable.

Lemma 111. *For any semiring $\mathbb{D}$ with a recursive underlying set and any integer $d \geq 1$, there exists a computable, injective morphism from $\mathbb{D}^{d\times d}$ to $\mathbb{D}^{(d+1)\times(d+1)}$.*

Proof. Map each $M \in \mathbb{D}^{d\times d}$ to $\begin{bmatrix} M & O \\ O & 1 \end{bmatrix}$. □

Let d and k be two positive integers. If $\text{Free}(k)\left[\mathbb{N}^{d\times d}\right]$ is undecidable then it follows from Lemma 111 that $\text{Free}(k)\left[\mathbb{N}^{e\times e}\right]$ is undecidable for every integer $e \geq d$. Table 1 summarizes our results on the decidability of $\text{Free}(k)\left[\mathbb{N}^{d\times d}\right]$ as (k,d) runs over $(\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0,1\})$. The table is to be understood as follows: if the symbol that occurs at the intersection of row d and column k is a "D" then $\text{Free}(k)\left[\mathbb{N}^{d\times d}\right]$ is decidable, if it is a "U" then the problem is undecidable, and if it is a "$\cdot$" then the decidability of the problem is still open.

Noteworthy is that Lemma 111 does not hold the other way round in general.

Proposition 112. *Let $\mathbb{D}$ be a semiring, let $\mathbb{K}$ be a field, and let d be an integer greater than one. There exists no injective morphism from $\mathbb{D}^{d\times d}$ to $\mathbb{K}^{(d-1)\times(d-1)}$.*

Proof. The proof is easily derived from the following two lemmas.

Lemma 113. *There exists $M \in \mathbb{D}^{d\times d}$ such that $M^d \neq M^{d-1}$ and $M^{d+1} = M^d$.*

Proof. Let $M \in \mathbb{D}^{d\times d}$ be as follows: for all indices i, $j \in [\![1, d]\!]$, the $(i,j)^{\text{th}}$ entry of M equals one if $j - i = 1$, and zero otherwise. It is easy to see that M^{d-1} has a one in its right-upper corner whereas both M^d and M^{d+1} are zero matrices. □

		k															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$\cdots$
d	2	D	·	·	·	·	·	·	·	·	·	·	·	·	·	·	$\cdots$
	3	D	·	·	·	·	·	·	·	·	·	·	·	U	U	U	$\cdots$
	4	D	·	·	·	·	·	·	·	·	·	·	·	U	U	U	$\cdots$
	5	D	·	·	·	·	·	·	·	·	·	·	·	U	U	U	$\cdots$
	6	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	$\cdots$
	7	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	$\cdots$
	8	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	$\cdots$
	9	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	$\cdots$
	10	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	$\cdots$
	11	D	·	·	·	·	·	U	U	U	U	U	U	U	U	U	$\cdots$
	12	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	13	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	14	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	15	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	16	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	17	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	18	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	19	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	20	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	21	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	22	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	23	D	·	·	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	24	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	25	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	26	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	27	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	28	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	29	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	30	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	31	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	32	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	33	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	34	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	35	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	36	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	37	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	38	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	39	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	40	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	41	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	42	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	43	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	44	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	45	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	46	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	47	D	·	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	48	D	U	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	49	D	U	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	50	D	U	U	U	U	U	U	U	U	U	U	U	U	U	U	$\cdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Table 1: Current knowledge about the decidability of $\textsc{Free}(k)\big[\mathbb{N}^{d\times d}\big]$ for all pairs (k, d).

Lemma 114. *For every $N \in \mathbb{K}^{(d-1)\times(d-1)}$, $N^d = N^{d-1}$ if and only if there exists $n \in \mathbb{N}$ such that $N^{n+1} = N^n$.*

Proof. The "only if part" of the statement is trivial. Let us now prove the "if part". Let $\mu(\mathsf{z})$ denote the minimal polynomial of N over $\mathbb{K}$. Assume that $N^{n+1} = N^n$. Now, $\mu(\mathsf{z})$ divides $\mathsf{z}^{n+1} - \mathsf{z}^n = \mathsf{z}^n(\mathsf{z} - 1)$. Since the degree of $\mu(\mathsf{z})$ is at most $d-1$, $\mu(\mathsf{z})$ divides in fact $\mathsf{z}^{d-1}(\mathsf{z}-1) = \mathsf{z}^d - \mathsf{z}^{d-1}$. From that we deduce $N^d = N^{d-1}$. □

Lemma 114 ensures that there does not exist any matrix $N \in \mathbb{K}^{(d-1)\times(d-1)}$ satisfying both $N^d \neq N^{d-1}$ and $N^{d+1} = N^d$. Combining the latter fact with Lemma 113 yields the proposition. □

To conclude the section, we put forth an interesting open question related to the decidability of $\mathrm{F{\small REE}}\big[\mathbb{Z}^{4\times 4}\big]$.

Open question 115 (Bell and Potapov [2])**.** *Denote by $\mathcal{L}$ the set of all four-by-four matrices of the form*

$$\begin{bmatrix} x & y & z & t \\ -y & x & t & -z \\ -z & -t & x & y \\ -t & z & -y & x \end{bmatrix}$$

with x, y, z, $t \in \mathbb{Z}$. Under usual matrix addition and multiplication, $\mathcal{L}$ is a ring, which is isomorphic to the ring of Lipschitz quaternions (or Hamiltonian integers). In particular $\mathcal{L}$ is a semigroup under matrix multiplication. The decidability of $\mathrm{F{\small REE}}\big[\mathcal{L}\big]$ *is open.*

Acknowledgments

The authors thank Juhani Karhumäki for his hospitality and Luc Guyot for his help in writing Section 6.2.2.

References

[1] A. F. Beardon. Pell's equation and two generator free Möbius groups. *Bulletin of the London Mathematical Society*, 25(6):527–532, 1993.

[2] P. Bell and I. Potapov. Reachability problems in quaternion matrix and rotation semigroups. In Luděk Kučera and Antonín Kučera, editors, *Proceedings of the 32nd International Symposium on Mathematical Foundations of Computer Science (MFCS'07)*, volume 4708 of *Lecture Notes in Computer Science*, pages 346–358. Springer, 2007.

[3] J. Berstel and D. Perrin. *Theory of codes.* Pure and Applied Mathematics. Academic Press, 1985.

[4] V. D. Blondel and V. Canterini. Undecidable problems for probabilistic automata of fixed dimension. *Theory of Computing Systems*, 36(3):231–245, 2003.

[5] V. D. Blondel, J. Cassaigne, and J. Karhumäki. Freeness of multiplicative matrix semigroups. In V. D. Blondel and A. Megretski, editors, *Unsolved problems in mathematical systems and control theory*, pages 309–314. Princeton University Press, 2004.

[6] V. D. Blondel and J. N. Tsitsiklis. When is a pair of matrices mortal? *Information Processing Letters*, 63(5):283–286, 1997.

[7] V. D. Blondel and J. N. Tsitsiklis. The boundedness of all products of a pair of matrices is undecidable. *Systems & Control Letters*, 41(2):135–140, 2000.

[8] O. Bournez and M. Branicky. The mortality problem for matrices of low dimensions. *Theory of Computing Systems*, 35(4):433–448, 2002.

[9] J. Cassaigne, T. Harju, and J. Karhumäki. On the undecidability of freeness of matrix semigroups. *International Journal of Algebra and Computation*, 9(3–4):295–305, 1999.

[10] J. Cassaigne and J. Karhumäki. Examples of undecidable problems for 2-generator matrix semigroups. *Theoretical Computer Science*, 204(1–2):29–34, 1998.

[11] C. Choffrut and J. Karhumäki. Some decision problems on integer matrices. *RAIRO – Theoretical Informatics and Applications*, 39(1):125–131, 2005.

[12] V. Claus. Some remarks on PCP(k) and related problems. *The Bulletin of the European Association for Theoretical Computer Science (EATCS)*, 12:54 – 61, 1980.

[13] A. Ehrenfeucht, J. Karhumäki, and G. Rozenberg. The (generalized) Post correspondence problem with lists consisting of two words is decidable. *Theoretical Computer Science*, 21(2):119–144, 1982.

[14] A. Ehrenfeucht and G. Rozenberg. On the (generalized) Post correspondence problem with lists of length 2. In S. Even and O. Kariv, editors, *Proceedings of the 8th International Colloquium on Automata, Languages and Programming (ICALP'81)*, volume 115 of *Lecture Notes in Computer Science*, pages 408–416. Springer, 1981.

[15] Z. Grunschlag. *Algorithms in Geometric Group Theory*. PhD thesis, Graduate division of the University of California at Berkeley, 1999.

[16] A. Grytczuk and M. Wójtowicz. Beardon's diophantine equations and non-free Möbius groups. *Bulletin of the London Mathematical Society*, 32(3):305–310, 2000.

[17] L. Guyot. Sur l'équation diophantienne $xyz^2 = t^2(xy - x - y - 1)$. Manuscript, 2008.

[18] V. Halava and T. Harju. Mortality in matrix semigroups. *The American Mathematical Monthly*, 108(7):649–653, 2001.

[19] V. Halava, T. Harju, and M. Hirvensalo. Binary (generalized) Post correspondence problem. *Theoretical Computer Science*, 276(1–2):183–204, 2002.

[20] V. Halava, T. Harju, and M. Hirvensalo. Undecidability bounds for integer matrices using Claus instances. *International Journal of Foundations of Computer Science*, 18(5):931–948, 2007.

[21] T. Harju and J. Karhumäki. Morphisms. In G. Rozenberg and A. Salomaa, editors, *Handbook of formal languages*, volume 1, pages 439–510. Springer, 1997.

[22] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to automata theory, languages, and computation.* Addison-Wesley, second edition, 2001.

[23] G. Jacob. La finitude des représentations linaires des semi-groupes est décidable. *Journal of Algebra*, 52(2):437–459, 1978.

[24] M. Kambites, P. V. Silva, and B. Steinberg. On the rational subset problem for groups. *Journal of Algebra*, 309(2):622–639, 2007.

[25] R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *Journal of the Association for Computing Machinery*, 33(4):808–821, 1986.

[26] D. A. Klarner, J.-C. Birget, and W. Satterfield. On the undecidability of the freeness of integer matrix semigroups. *International Journal of Algebra and Computation*, 1(2):223–226, 1991.

[27] M. Krom and M. Krom. More on mortality. *The American Mathematical Monthly*, 97(1):37–38, 1990.

[28] M. V. Lawson. *Finite automata.* CRC Press, 2003.

[29] M. Lothaire. *Combinatorics on words.* Cambridge Mathematical Library. Cambridge University Press, second edition, 1997.

[30] M. Lothaire. *Algebraic combinatorics on words.* Number 90 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2002.

[31] R. C. Lyndon and P. E. Schupp. *Combinatorial group theory*, volume 89 of *Ergebnisse der Mathematik und ihrer Grenzgebiete.* Springer, 1977.

[32] A. Mandel and I. Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5(2):101–111, 1977.

[33] Y. Matiyasevich and G. Sénizergues. Decision problems for semi-Thue systems with a few rules. *Theoretical Computer Science*, 330(1):145–169, 2005.

[34] F. Mazoit. Autour de quelques problèmes de décidabilité sur des semigroupes de matrices. Unpublished, 1998.

[35] F. Nicolas. (Generalized) Post correspondence problem and semi-Thue systems. Available at `http://arxiv.org/abs/0802.0726`, 2007.

[36] M. S. Paterson. Unsolvability in 3×3 matrices. *Studies in Applied Mathematics*, XLIX(1):105–107, 1970.

[37] E. L. Post. A variant of a recursively unsolvable problem. *Bulletin of the American Mathematical Society*, 52(4):264–268, 1946.

[38] W. Rytter. The space complexity of the unique decipherability problem. *Information Processing Letters*, 23(1):1–3, 1986.

[39] J. Sakarovitch. *Élements de théorie des automates*. Vuibert, 2003.

[40] A. Salomaa. *Jewels of formal language theory*. Computer Science Press, 1981.

[41] A. A. Sardinas and G. W. Patterson. A necessary and sufficient condition for the unique decomposition of coded messages. In IRE Convention Record, Part 8, pages 104–108, 1953.

[42] P. Schultz. Mortality of 2×2 matrices. *The American Mathematical Monthly*, 84(6):463–464, 1977.

[43] A. W. Strzeboński. Computing in the field of complex algebraic numbers. *Journal of Symbolic Computation*, 24(6):647–656, 1997.

[44] J. W. Wamsley. On certain pairs of matrices which generate free groups. *Bulletin of the London Mathematical Society*, 5(1):109–110, 1973.